

System Functional (Admin & Control) RVTM

SFR1088: NGI shall send a Link Maintenance request to the appropriate External System when an Identity containing an external link is deleted.

BIO.FEAT274: Upon data removal by the owning agency for records retention policy purposes, the solution shall remove that data from in-scope systems within 24 hours.

BIO.FEAT275: When CJIS executes a removal for an individual, US-VISIT shall unlink the FBI criminal history and all references to that criminal history from any DHS encounters for that individual.

SFR1089: NGI shall include the deleted UCN and External System Identifier as part of a Link Maintenance request.

SFR1090: NGI shall send a Link Maintenance request indicating deletion to an External System in accordance with the latest EBTS version.

BIO.FEAT129: The solution shall employ biometric standards established by the National Institute of Standards and Technology (NIST), i.e. the ANSI National Standard for Information Systems -- Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information, ANSI/NIST-ITL-1-2007.

BIO.FEAT182: The solution shall employ a standard format for query responses.

BIO.FEAT194: The solution shall support EBTS compliant data exchange.

SFR1091: NGI shall accept a Link Maintenance response from an External System in accordance with the latest EBTS version.

BIO.FEAT129: The solution shall employ biometric standards established by the National Institute of Standards and Technology (NIST), i.e. the ANSI National Standard for Information Systems -- Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information, ANSI/NIST-ITL-1-2007.

BIO.FEAT194: The solution shall support EBTS compliant data exchange.

SFR1092: NGI shall perform exception processing when a Link Maintenance request is rejected by an External System.

SFR1421: NGI shall allow an Authorized FBI System Administrator access to a centralized system status reporting service.

LEG.FR402: IAFIS shall allow Authorized FBI System Administrators access to system status and reporting capabilities.

STRQ932: IAFIS shall provide the ability for CJIS personnel to check the status of the systems.

SFR1422: NGI shall allow an Authorized FBI Service Provider access to a centralized system status reporting service.

SFR1423: NGI shall provide a centralized system status reporting service.

STRQ932: IAFIS shall provide the ability for CJIS personnel to check the status of the systems.

SFR1424: NGI shall provide parameter-based system status reporting capabilities.

SFR1425: NGI shall provide pre-defined system status reporting capabilities.

SFR1426: NGI shall collect system status data (e.g., readiness, utilization, queue status) for system components.

LEG.FR403: IAFIS shall collect system status data (i.e., readiness, utilization, queue status) for system components.

SFR1427: NGI shall collect system performance data (e.g., response times, workload).

LEG.FR404: IAFIS shall collect system performance data (i.e., response times, workload).

SFR1428: NGI shall provide system status reporting capabilities on each active system environment (e.g., operational, development, test).

LEG.FR405: IAFIS shall report system status information on each active system environment (i.e., operational, development support, and test support).

SFR1429: NGI shall provide system performance reporting capabilities on each active system environment (e.g., operational, development, test).

LEG.FR406: IAFIS shall report system performance information on each active system environment (i.e., operational, development support, and test support).

SFR1430: NGI shall retain system status data.

LEG.FR407: IAFIS shall retain system status data.

SFR1431: NGI shall retain system performance data.

LEG.FR408: IAFIS shall retain system performance data.

SFR1432: NGI shall provide the capability to maintain authorization rules (i.e., read/write/delete access) for all Identity History activities.

LEG.FR409: IAFIS shall maintain authorization rules (i.e., read/write/delete access) for all Subject Criminal History activities.

SFR1433: NGI shall provide the capability to maintain authorization rules (i.e., read/write/delete access) for all fingerprint maintenance activities.

BIO.FEAT307: The solution shall exclude the sharing of protected identities, undercover agents, protected witnesses, certain known or suspected terrorist subjects protected under Memorandum of Agreements with host countries and a portion of civilian type of IAFIS records.

LEG.FR410: IAFIS shall maintain authorization rules (i.e., read/write/delete access) for all Fingerprint maintenance activities.

STRQ131: IAFIS shall provide the ability to electronically access the military database files.

STRQ130: IAFIS shall provide the ability to electronically access the military database files.

STRQ997: IAFIS shall make military fingerprint records accessible for search.

SFR1434: NGI shall provide the capability to maintain authorization rules (i.e., read/write/delete access) for all Latent maintenance activities.

LEG.FR411: IAFIS shall maintain authorization rules (i.e., read/write/delete access) for all Latent maintenance activities.

SFR1435: NGI shall provide the capability to maintain rules regarding who will be permitted to access (e.g., search, retrieve) the criminal repository.

STRQ447: IAFIS shall provide access to all type-2 arrest and disposition data for latent match candidates.

SFR1436: NGI shall provide the capability to maintain rules regarding who will be permitted to access (e.g., search, retrieve) the civil repository.

STRQ447: IAFIS shall provide access to all type-2 arrest and disposition data for latent match candidates.

STRQ896: The system shall communicate civil criminal history check responses to the submitting channeling institution (e.g., ABA and OPM) electronically.

STRQ895: The system shall route civil criminal history check responses back to the submitting non-government channeling institution (e.g., ABA) for distribution to the original submitter.

STRQ1029: IAFIS shall allow controlled access to civil information.

STRQ1114: IAFIS shall allow for law enforcement agency only access to certain civil records based on a flag.

SFR1437: NGI shall provide the capability to maintain rules regarding who will be permitted to access (e.g., search, retrieve) the RISC.

STRQ447: IAFIS shall provide access to all type-2 arrest and disposition data for latent match candidates.

SFR1438: NGI shall provide the capability to maintain rules regarding who will be permitted to access (e.g., search, retrieve) an unsolved biometric file.

STRQ447: IAFIS shall provide access to all type-2 arrest and disposition data for latent match candidates.

SFR1439: NGI shall provide the capability to maintain rules regarding who will be permitted to access (e.g., search, retrieve) an SPC File.

SFR1440: NGI shall provide the capability to maintain rules regarding who will be permitted to access (e.g., search, retrieve) a newly created NGI repository.

SFR1441: NGI shall support Authorized FBI Service Provider workgroup assignments.

LEG.FR412: IAFIS shall support FBI Service Provider workgroup assignments.

SFR1442: NGI shall allow Authorized ITF Contributors to perform maintenance on only their Identity data.

SFR1443: NGI shall allow an Authorized External System to perform maintenance on only their Identity data.

BIO.FEAT63: The solution shall provide the ability for the owning agency to electronically modify biometric information on existing records based on a confirmed biometric identification.

BIO.FEAT65: The solution shall provide the ability for the data owning agency to electronically update biographic information.

SFR1445: NGI shall allow Authorized Contributors to perform Identity maintenance on only their Identity data.

BIO.FEAT63: The solution shall provide the ability for the owning agency to electronically modify biometric information on existing records based on a confirmed biometric identification.

BIO.FEAT65: The solution shall provide the ability for the data owning agency to electronically update biographic information.

LEG.FR582: IAFIS shall reject an Unsolved Latent File Delete Request when the requestor is not the owner of the ULF record.

SFR1446: NGI shall allow Authorized FBI Service Providers to perform Identity maintenance on all Identity data.

SFR1447: NGI shall allow Authorized Contributors to perform photo maintenance on their own photos.

LEG.FR583: IAFIS shall reject a Photo Image Delete Request when the Contributor of the request is not the owner of the photo set.

SFR1448: NGI shall allow Authorized FBI Service Providers to perform photo maintenance on all photos.

SFR1449: NGI shall allow Authorized Contributors to perform palmprint maintenance on their own palmprints.

SFR1450: NGI shall allow Authorized FBI Service Providers to perform palmprint maintenance on all palmprints.

SFR1451: NGI shall allow Authorized Contributors to perform supplemental fingerprint and palmprint maintenance on their own supplemental fingerprint and palmprint information.

SFR1452: NGI shall allow Authorized FBI Service Providers to perform supplemental fingerprint and palmprint maintenance on all Supplemental Fingerprint and Palmprint information.

SFR1453: NGI shall allow Authorized Contributors to perform iris maintenance on their own iris data.

SFR1454: NGI shall allow Authorized FBI Service Providers to perform iris maintenance on all iris data.

SFR1455: NGI shall allow Authorized Contributors to perform Rap Back maintenance on their own Rap Back subscriptions.

STRQ1062: IAFIS shall provide automated maintenance to the states for RAP BACK.

SFR1456: NGI shall allow Authorized FBI Service Providers to perform Rap Back maintenance on all Rap Back subscriptions.

STRQ1062: IAFIS shall provide automated maintenance to the states for RAP BACK.

SFR1457: NGI shall allow Authorized Contributors to perform Rap Back subscription renewal on their own Rap Back subscriptions.

SFR1458: NGI shall allow Authorized FBI Service Providers to perform Rap Back subscription renewal on all Rap Back subscriptions.

SFR1459: NGI shall reject requests from Authorized Contributors who do not have valid authorization to perform requested system services.

SFR1460: NGI shall apply dissemination rules to all NGI Responses.

BIO.FEAT46: The solution shall enable authorized personnel to disassociate the biographic data of an enumerated individual from the stored biometrics for the individual if that individual belongs to a special category such as protected witnesses and under cover agents.

BIO.FEAT141: The solution shall provide authorized users real-time access to all information entered or updated in the system based on user permissions.

BIO.FEAT227: The solution shall provide enumerators only to requesting agencies that have agreements with US-VISIT detailing the terms and conditions for using and disseminating enumerators.

LEG.FR414: IAFIS shall apply dissemination rules to all IAFIS responses.

LEG.FR415: IAFIS shall maintain dissemination rules for all Subject Criminal History responses.

LEG.FR416: IAFIS shall maintain dissemination rules for all fingerprint responses.

LEG.FR417: IAFIS shall maintain dissemination rules for all Latent responses.

SFR1461: NGI shall apply dissemination rules to all NGI Notifications.

- BIO.FEAT46: The solution shall enable authorized personnel to disassociate the biographic data of an enumerated individual from the stored biometrics for the individual if that individual belongs to a special category such as protected witnesses and under cover agents.
- BIO.FEAT80: The solution shall provide the ability to notify the owner of a biometrically verified record when criminal information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).
- BIO.FEAT87: The solution shall provide the ability to notify the owner of a biometrically verified record when civil information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).
- LEG.FR413: IAFIS shall apply dissemination rules to all IAFIS notifications.
- STRQ519: The Enhanced IAFIS Repository shall provide expanded capabilities that implement Federal, State, and local rules and choices governing dissemination
- STRQ516: The Enhanced IAFIS Repository shall provide expanded capabilities that implement Federal, State, and local rules and choices governing submission, retention, and dissemination of civil data.
- STRQ665: IAFIS shall allow registration of informants into Rap Back with a special stop to prevent any dissemination without a call first to registering agency.
- STRQ808: Rap Back shall not violate privacy issues.
- STRQ890: IAFIS shall ensure to limit the dissemination of civil data of Special Stops subjects when consolidating criminal and civil data.
- SFR1462: NGI shall provide the capability to maintain dissemination rules for information contained in the criminal repository.**
- SFR1463: NGI shall provide the capability to maintain dissemination rules for information contained in the civil repository.**
- STRQ97: Non criminal history information shall not be disseminated for civil submissions.
- STRQ98: Non criminal history information shall not be disseminated for civil submissions, but reported to holder of record information.
- STRQ519: The Enhanced IAFIS Repository shall provide expanded capabilities that implement Federal, State, and local rules and choices governing dissemination of civil data.
- STRQ516: The Enhanced IAFIS Repository shall provide expanded capabilities that implement Federal, State, and local rules and choices governing submission, retention, and dissemination of civil data.
- STRQ890: IAFIS shall ensure to limit the dissemination of civil data of Special Stops subjects when consolidating criminal and civil data.
- STRQ896: The system shall communicate civil criminal history check responses to the submitting channeling institution (e.g., ABA and OPM) electronically.
- STRQ895: The system shall route civil criminal history check responses back to the submitting non-government channeling institution (e.g., ABA) for distribution to the original submitter.
- STRQ1029: IAFIS shall allow controlled access to civil information.
- STRQ1114: IAFIS shall allow for law enforcement agency only access to certain civil records based on a flag.
- SFR1464: NGI shall provide the capability to maintain dissemination rules in support of a RISC multi-tiered shared data infrastructure.**
- BIO.FEAT80: The solution shall provide the ability to notify the owner of a biometrically verified record when criminal information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).
- BIO.FEAT87: The solution shall provide the ability to notify the owner of a biometrically verified record when civil information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).
- SFR1465: NGI shall provide the capability to maintain dissemination rules for information in an SPC File.**
- SFR1466: NGI shall provide the capability to maintain dissemination rules for information contained in a newly created NGI repository.**
- SFR1467: NGI shall provide the capability to maintain dissemination rules for all photo responses.**
- SFR1469: NGI shall provide the capability to maintain dissemination rules for all palmprint responses.**
- SFR1470: NGI shall provide the capability to maintain dissemination rules for all supplemental fingerprint and palmprint responses.**

SFR1471: NGI shall provide the capability to maintain dissemination rules for all iris responses.

SFR1472: NGI shall provide the capability to maintain dissemination rules for all fingerprint responses.

BIO.FEAT307: The solution shall exclude the sharing of protected identities, undercover agents, protected witnesses, certain known or suspected terrorist

SFR1473: NGI shall provide the capability to maintain dissemination rules for all Tenprint Identification Search responses.

BIO.FEAT80: The solution shall provide the ability to notify the owner of a biometrically verified record when criminal information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).

BIO.FEAT87: The solution shall provide the ability to notify the owner of a biometrically verified record when civil information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).

SFR1474: NGI shall provide the capability to maintain dissemination rules for all Fingerprint Verification responses.

BIO.FEAT80: The solution shall provide the ability to notify the owner of a biometrically verified record when criminal information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).

BIO.FEAT87: The solution shall provide the ability to notify the owner of a biometrically verified record when civil information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).

SFR1475: NGI shall provide the capability to maintain dissemination rules for International Terrorist Identification Search responses based upon a multi-tiered shared data structure.

SFR1476: NGI shall provide the capability to maintain dissemination rules for all Latent Fingerprint Investigation Search responses.

BIO.FEAT80: The solution shall provide the ability to notify the owner of a biometrically verified record when criminal information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).

BIO.FEAT87: The solution shall provide the ability to notify the owner of a biometrically verified record when civil information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).

SFR1477: NGI shall provide the capability to maintain dissemination rules for all Latent Print Search responses.

BIO.FEAT80: The solution shall provide the ability to notify the owner of a biometrically verified record when criminal information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).

BIO.FEAT87: The solution shall provide the ability to notify the owner of a biometrically verified record when civil information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).

SFR1478: NGI shall provide the capability to maintain dissemination rules for all Immigration Violator File Notifications.

BIO.FEAT80: The solution shall provide the ability to notify the owner of a biometrically verified record when criminal information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).

BIO.FEAT87: The solution shall provide the ability to notify the owner of a biometrically verified record when civil information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).

SFR1479: NGI shall provide the capability to maintain dissemination rules for all Want Notifications.

BIO.FEAT80: The solution shall provide the ability to notify the owner of a biometrically verified record when criminal information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).

BIO.FEAT87: The solution shall provide the ability to notify the owner of a biometrically verified record when civil information is received on that individual, without notifying the querying officer that the hit has occurred (i.e. silent hit).

SFR1480: NGI shall provide the capability to maintain dissemination rules for all Latent Decision Notifications.

BIO.FEAT322: The solution shall accommodate the Transaction-Volume spreadsheet version 5.0 dated April 16, 2009.

SFR1481: NGI shall provide the capability to maintain dissemination rules for all Special Processing Flag Notifications.

SFR1482: NGI shall provide the capability to maintain dissemination rules for all Consolidation Notifications.

- SFR1483:** NGI shall provide the capability to maintain dissemination rules for all Rap Back Renewal Notifications.
- SFR1484:** NGI shall provide the capability to maintain dissemination rules for all Rap Back Notifications.
- SFR1485:** NGI shall provide the capability to maintain dissemination rules for information in an unsolved biometric file.
- SFR1486:** NGI shall provide the capability to maintain dissemination rules for all Identity History responses.
- SFR1487:** NGI shall provide the capability to maintain dissemination rules for all Investigation Search responses.
- SFR1488:** NGI shall provide the capability to maintain dissemination rules for all Linked Record Activity Notifications.
- SFR1489:** NGI shall provide the capability to maintain dissemination rules for all External System Linked Record Activity Notifications.
- SFR1493:** NGI shall perform maintenance of Identity history contained within the NGI Repositories as a result of fingerprint identification searches in
LEG.FR418: IAFIS shall perform maintenance of subject criminal history contained within the IAFIS Repositories as a result of fingerprint identification searches in accordance with Table 3-1: File Maintenance Rules.
- SFR1494:** NGI shall perform maintenance of biometric information contained within the NGI Repositories as a result of fingerprint identification searches in accordance with Table 3-1 File Maintenance Rules.
LEG.FR419: IAFIS shall perform maintenance of fingerprint information contained within the IAFIS Repositories as a result of fingerprint identification searches in accordance with Table 3-1: File Maintenance Rules.
- SFR1495:** NGI shall maintain Identity information as a result of Identity maintenance requests in accordance with Table 3-1 File Maintenance Rules.
- SFR1496:** NGI shall provide the capability to maintain rules regarding enrollment into the criminal repository.
- SFR1497:** NGI shall provide the capability to maintain rules regarding enrollment into the civil repository.
- SFR1498:** NGI shall provide the capability to maintain enrollment rules regarding who will be permitted to enter information into an unsolved biometric file.
- STRQ390: EIR shall provide access to the civil SLC files to non-federal agencies per special request.
- SFR1499:** NGI shall provide the capability to maintain enrollment rules regarding who will be permitted to enter information into an SPC File.
- SFR1500:** NGI shall provide the capability to maintain enrollment rules regarding what types of records may be included in the RISC.
- SFR1501:** NGI shall provide the capability to maintain enrollment rules regarding who will be permitted to enter information into the RISC.
- SFR1502:** NGI shall enroll records to the RISC when record type satisfies enrollment rules for RISC.
- SFR1503:** NGI shall delete records from the RISC when record type no longer satisfies enrollment rules for RISC.
- SFR1504:** NGI shall provide the capability to maintain enrollment rules for a newly created NGI repository.
- SFR1505:** NGI shall provide event information as part of the Identity History Summary.
LEG.FR422: IAFIS shall provide event information as part of the Subject Criminal History Rap Sheet
- SFR1506:** NGI shall provide a UCN as part of the Identity History Summary.
BIO.FEAT370: The solution shall provide an unique identifier other than the FNU for each fingerprint image shared.
BIO.FEAT371: The solution shall exclude the FNU for each fingerprint image shared.
BIO.FEAT373: The solution shall provide the capability to access Criminal History Record Information based on the unique identifier provided for shared fingerprint images.
LEG.FR420: IAFIS shall provide an FNU as part of a Subject Criminal History Rap Sheet.
- SFR1507:** NGI shall provide an external system link identifier(s) (e.g., FIN, NIC) as part of the Identity History Summary.
BIO.FEAT227: The solution shall provide enumerators only to requesting agencies that have agreements with US-VISIT detailing the terms and conditions for using and disseminating enumerators.
SUR45: NGI shall provide external system link identifiers as part of Identity History responses.
SUR43: NGI shall support the retrieval of Identity History information.

LEG.UR11: IAFIS shall support Criminal History Information Requests containing a unique identifier.
LEG.UR12: IAFIS shall support Civil History Information Requests containing a unique identifier.
STRQ100: The System shall send back all information on the Criminal Justice applicants, retained by the FBI, to the original request
STRQ99: The system shall send back all information (criminal history, wanted, suspected terrorists, etc) on Criminal Justice applicants retained by the FBI, for both original request and Rap Back.
STRQ104: IAFIS shall be able to send all responses (criminal, civil, rap back) directly to originating requestor in addition to responses being sent to SIB
STRQ102: IAFIS shall be able to send all responses (criminal, civil, rap back) directly to originating requestor in addition to responses being sent to SIB
STRQ515: The Enhanced IAFIS repository shall provide a full range of civil search and response services associated with criminal file activity plus access to civil data (e.g., CRN, subject descriptors, contributing agency, reason fingerprinted, and civil history).
STRQ993: IAFIS shall make military fingerprint records accessible for search.
STRQ992: IAFIS shall make military and ICE fingerprint records accessible for search.
STRQ998: IAFIS shall make military fingerprint records accessible for search.
STRQ995: IAFIS shall make ICE fingerprint records accessible for search.
STRQ992: IAFIS shall make military and ICE fingerprint records accessible for search.
STRQ1136: IAFIS shall provide the ability to electronically access the military database files.
STRQ132: IAFIS shall provide the ability to electronically access the military database files.
STRQ130: IAFIS shall provide the ability to electronically access the military database files.
STRQ1134: IAFIS shall have the capability to convert Military records into an electronic civil file and automate the retrieval of these records.

SFR1508: NGI shall provide active Want information as part of the Identity History Summary

LEG.FR423: IAFIS shall provide active want information as part of the Subject Criminal History Rap Sheet.
SUR24: NGI shall provide wanted person information with the Tenprint Fingerprint Identification Search response.
LEG.UR5: IAFIS shall provide wanted person information with the Tenprint Fingerprint Identification Search Response.
SUR23: NGI shall provide an appropriate response to a Tenprint Fingerprint Identification Search request.
LEG.UR4: IAFIS shall provide an appropriate response to a Tenprint Fingerprint Identification Search request.
SUR1: NGI shall support Tenprint Fingerprint Identification Search requests.
LEG.UR1: IAFIS shall support Tenprint Fingerprint Identification Search requests.

SFR1509: NGI shall provide active Flash information as part of the Identity History Summary

LEG.FR424: IAFIS shall provide active Flash information as part of the Subject Criminal History Rap Sheet.
SUR25: NGI shall provide flash information with the Tenprint Fingerprint Identification Search response.
LEG.UR6: IAFIS shall provide flash information with the Tenprint Fingerprint Identification Search Response.
SUR23: NGI shall provide an appropriate response to a Tenprint Fingerprint Identification Search request.
LEG.UR4: IAFIS shall provide an appropriate response to a Tenprint Fingerprint Identification Search request.
SUR1: NGI shall support Tenprint Fingerprint Identification Search requests.
LEG.UR1: IAFIS shall support Tenprint Fingerprint Identification Search requests.

SFR1510: NGI shall provide active SOR information as part of the Identity History Summary.

LEG.FR425: IAFIS shall provide active SOR information as part of the Subject Criminal History Rap Sheet.

SUR26: NGI shall provide sex offender registry information with the Tenprint Fingerprint Identification Search response.

LEG.UR7: IAFIS shall provide sex offender registry information with the Tenprint Fingerprint Identification Search Response.

SUR23: NGI shall provide an appropriate response to a Tenprint Fingerprint Identification Search request.

LEG.UR4: IAFIS shall provide an appropriate response to a Tenprint Fingerprint Identification Search request.

SUR1: NGI shall support Tenprint Fingerprint Identification Search requests.

LEG.UR1: IAFIS shall support Tenprint Fingerprint Identification Search requests.

SFR1511: NGI shall provide Identity Theft information as part of the Identity History Summary.

STRQ946: IAFIS shall support a voluntary identity theft prevention file.

SUR27: NGI shall provide Identity Theft information with the Tenprint Fingerprint Identification Search response.

SUR23: NGI shall provide an appropriate response to a Tenprint Fingerprint Identification Search request.

LEG.UR4: IAFIS shall provide an appropriate response to a Tenprint Fingerprint Identification Search request.

SUR1: NGI shall support Tenprint Fingerprint Identification Search requests.

LEG.UR1: IAFIS shall support Tenprint Fingerprint Identification Search requests.

SFR1512: NGI shall provide an IVF indicator as part of the Identity History Summary.

BIO.FEAT397: The solution shall be able to provide notification to the submitting agency of a biometrically confirmed match on a subject referenced within the Immigration Violator File (IVF).

SFR1513: NGI shall indicate, on an Identity History Summary, whether or not photos are available for the specified subject.

SFR1514: NGI shall indicate, on an Identity History Summary, whether or not iris data is available for the specified subject.

STRQ647: IAFIS shall have a flag indicating iris data is available.

SFR1515: NGI shall indicate, on an Identity History Summary, whether or not palmprints are available for the specified subject.

SFR1516: NGI shall indicate, on an Identity History Summary, whether or not supplemental fingerprint and palmprint data is available for the specified subject.

SFR1517: NGI shall provide the capability to maintain business rules to support AQC of textual data as part of a Tenprint Fingerprint Identification Search.

LEG.FR426: IAFIS shall maintain business rules to support the Automated Quality Check (AQC) of textual data as part of a Tenprint fingerprint Identification Search.

SFR1518: NGI shall support, and the CJIS Division will make publicly available, fingerprint image quality threshold for fingerprint retention based upon image quality standards required in the latest version of the EBTS.

LEG.FR427: IAFIS shall support, and the CJIS Division will make publicly available, fingerprint image quality threshold for fingerprint retention.

SFR1519: NGI shall support, and the CJIS Division will make publicly available, a fingerprint image quality threshold for fingerprint searching based upon image quality standards required in the latest version of the EBTS.

LEG.FR428: IAFIS shall support, and the CJIS Division will make publicly available, fingerprint image quality threshold for fingerprint searches.

SFR1520: NGI shall support a fingerprint image quality improvement threshold.

STRQ419: IAFIS shall provide for increased ten-print fingerprint image quality.

SFR1521: NGI shall support various fingerprint image resolutions in accordance with the latest EBTS version (e.g., 500ppi, 1000ppi).

LEG.FR663: IAFIS shall accept fingerprint images at 1000ppi from Authorized Contributors as part of a Tenprint Fingerprint Identification Search request.

STRQ583: IAFIS shall target the compression ratio to no more than 10:1 for JPEG 2000 images.

STRQ582: IAFIS shall target the compression ratio to no more than 10:1 for JPEG 2000 and 15:1 for WSQ images.

- STRQ584: IAFIS shall target the compression ratio to no more than 10:1 for WSQ images.
- STRQ582: IAFIS shall target the compression ratio to no more than 10:1 for JPEG 2000 and 15:1 for WSQ images.
- STRQ587: For flat fingerprints taken on a platen (recording image) of 1 inch by 1 inch or smaller, the maximum compression ratio should be no more than 7:1 WSQ.
- STRQ586: For flat fingerprints taken on a platen (recording image) of 1 inch by 1 inch or smaller, the maximum compression ratio should be no more than 7:1 WSQ or JPEG 2000.
- STRQ588: For flat fingerprints taken on a platen (recording image) of 1 inch by 1 inch or smaller, the maximum compression ratio should be no more than JPEG 2000.
- STRQ586: For flat fingerprints taken on a platen (recording image) of 1 inch by 1 inch or smaller, the maximum compression ratio should be no more than 7:1 WSQ or JPEG 2000.
- STRQ613: IAFIS shall accept variable resolution for fingerprint storage.
- STRQ612: IAFIS shall accept variable resolution for fingerprint and latent prints for storage and searching.
- STRQ614: IAFIS shall accept variable resolution for fingerprint searching.
- STRQ612: IAFIS shall accept variable resolution for fingerprint and latent prints for storage and searching.
- STRQ615: IAFIS shall accept variable resolution for latent prints for storage.
- STRQ612: IAFIS shall accept variable resolution for fingerprint and latent prints for storage and searching.
- STRQ616: IAFIS shall accept variable resolution for latent prints for searching.
- STRQ612: IAFIS shall accept variable resolution for fingerprint and latent prints for storage and searching.
- STRQ1009: IAFIS shall provide the ability to store standard fingerprints at a 1000ppi.
- STRQ1007: IAFIS shall provide increased resolution of 1000 ppi for standard ten-print fingerprints.
- STRQ1008: IAFIS shall provide the ability to store and process standard fingerprints at a 1000ppi.
- STRQ1010: IAFIS shall provide the ability to process standard fingerprints at a 1000ppi.
- STRQ1007: IAFIS shall provide increased resolution of 1000 ppi for standard ten-print fingerprints.
- STRQ1008: IAFIS shall provide the ability to store and process standard fingerprints at a 1000ppi.
- STRQ1011: IAFIS shall set a minimum of 1000 ppi for submission of fingerprint latent prints for type-13 records.
- STRQ1015: AFIT shall support 500 ppi.
- STRQ2: AFIT and NPPS shall support 500 and 1000 ppi.
- STRQ1014: IAFIS shall allow fingerprint image quality ranging from 500 to 1000ppi.
- STRQ1016: AFIT shall support 1000 ppi.
- STRQ2: AFIT and NPPS shall support 500 and 1000 ppi.
- STRQ1014: IAFIS shall allow fingerprint image quality ranging from 500 to 1000ppi.
- SFR1522: Deleted.**
- SFR1523: Deleted.**
- SFR1524: NGI shall provide the capability to maintain minimum fingerprint match thresholds to support III/Verify function.**
- LEG.FR429: IAFIS shall maintain a minimum fingerprint match thresholds to support III/Verify function.
- SFR1525: NGI shall support fingerprint image compression algorithm in accordance with the latest version of the EBTS.**
- LEG.FR430: IAFIS shall support fingerprint image compression algorithm in accordance with the EBTS.
- SFR1526: NGI shall provide the capability to maintain a high confidence threshold to support automated FIC.**
- BIO.FEAT19: The solution shall provide the ability for automated 10-print positive identification.
- BIO.FEAT126: The solution shall provide the ability for human-confirmed 10 print positive identification.

- LEG.FR431: IAFIS shall maintain a Fingerprint Image Compare (FIC) high confidence threshold to support automated Tenprint Fingerprint Identification Search.
- LEG.FR643: IAFIS shall provide the capability to maintain a shared data high confidence threshold to support automated comparison processes against candidates identified in a shared data search.
- SFR1527: NGI shall provide the capability to maintain a low confidence threshold to support automated FIC.**
- BIO.FEAT126: The solution shall provide the ability for human-confirmed 10 print positive identification.
- LEG.FR432: IAFIS shall maintain a Fingerprint Image Compare (FIC) low confidence threshold to support Tenprint Fingerprint Identification Search.
- LEG.FR644: IAFIS shall provide the capability to maintain a shared data low confidence threshold to support the automated comparison processes against candidates identified in a shared data search.
- SFR1528: NGI shall provide the capability to maintain external system response time thresholds.**
- SFR1529: NGI shall provide 95% segmentation accuracy of the plain impression in support of the Automated Fingerprint Sequence Check Service (e.g., produce highly matchable images, identify finger positions, detect segmentation failures).**
- STRQ229: IAFIS shall accept electronic submissions because the quality of the images will be better than paper cards.
- SFR1530: NGI shall provide the capability to maintain fingerprint image quality standards.**
- SFR1531: NGI shall provide the capability to maintain latent fingerprint image quality standards.**
- SFR1532: NGI shall provide the capability to maintain latent print image quality standards.**
- SFR1533: NGI shall support, and the CJIS Division will make publicly available, photo image quality thresholds for facial recognition based upon image quality standards required in the latest EBTS version.**
- STRQ118: IAFIS shall establish a photo image quality measure for any photo type accepted for storage in IAFIS.
- STRQ1150: The FBI shall set a standard for sending in photos and define the required quality needed in sending them.
- STRQ403: The NGI solution will be based on open standards
- SFR1534: NGI shall support, and the CJIS Division will make publicly available, palmprint image quality thresholds for search based upon image quality standards required in the latest EBTS version.**
- STRQ403: The NGI solution will be based on open standards
- SFR1535: NGI shall support, and the CJIS Division will make publicly available, supplemental fingerprint and palmprint image quality thresholds for search based upon image quality standards required in the latest EBTS version.**
- STRQ403: The NGI solution will be based on open standards
- SFR1536: NGI shall support, and the CJIS Division will make publicly available, iris image quality reject thresholds for search based upon iris image quality standards required in the latest EBTS version.**
- SFR1537: NGI shall delete the oldest record from the ULF, when the ULF is at maximum capacity and a new record is received for enrollment.**
- LEG.FR433: IAFIS shall delete the oldest record from the ULF, when ULF is at maximum capacity and a new record is received for enrollment.
- SFR1538: NGI shall support a palmprint feature extraction method that is publicly available.**
- SFR1539: NGI shall maintain a unique identity across the multiple repositories (e.g., criminal, civil, RISC, unsolved biometric files).**
- BIO.FEAT39: The solution shall associate all biographic information captured during previous interactions to the enumerator, FNU, and/or CRN of that individual.
- BIO.FEAT43: The solution shall associate biometrically-confirmed criminal information to the enumerator and/or FNU.
- BIO.FEAT44: The solution shall associate biometrically-confirmed civil background information to the enumerator and/or CRN.
- BIO.FEAT69: The solution shall always associate any updated information (biometrics, biographics, source of biographical information, individual's role, criminal history, civil background history) to the enumerator, FNU, and/or CRN of that individual.
- BIO.FEAT163: The solution shall provide the capability to search all biometrics in the solution prior to enrollment of a new subject.

BIO.FEAT229: The solution shall retain one identity for one person in each system (IDENT and IAFIS) subject to TAR/FAR requirements.
BIO.FEAT281: The solution shall associate all biographic information captured during previous interactions to the enumerator and/or FNU of that individual.

BIO.FEAT304: The solution shall update retained records automatically when subject information is added.
BIO.FEAT305: The solution shall update retained records automatically when subject information is updated.
BIO.FEAT306: The solution shall update retained records automatically when subject information is deleted.
BIO.FEAT340: The solution shall provide notification of all newly enrolled in-scope IDENT records, to include biometrics and identifiers to the IAFIS.
BIO.FEAT370: The solution shall provide a unique identifier other than the FNU for each fingerprint image shared.
BIO.FEAT371: The solution shall exclude the FNU for each fingerprint image shared.
BIO.FEAT373: The solution shall provide the capability to access Criminal History Record Information based on the unique identifier provided for shared fingerprint images.

SFR1540: NGI shall provide the capability for storing multiple occurrences up to a maximum number of biographic identifiers in each Identity History Record.

LEG.FR434: IAFIS shall provide the capability for storing multiple occurrences up to the maximum number of name, social security number, scars, marks, and tattoos, miscellaneous numbers, and dates of birth in each Subject Criminal History Record.

SFR1541: NGI shall support the synchronization of Identity History Data in accordance with the III/NFF Operational and Technical Manual.

LEG.FR435: IAFIS shall support the synchronization of III subject criminal history data in accordance with the III/NFF Operations and Technical Manual.

SFR1542: NGI shall provide the capability to perform inter-repository searches to identify potential Identity consolidations.

BIO.FEAT163: The solution shall provide the capability to search all biometrics in the solution prior to enrollment of a new subject.
BIO.FEAT336: The solution shall perform an initial comparison of the in-scope biometric records contained in IDENT with the in-scope biometric records contained in IAFIS.
BIO.FEAT337: The solution shall include the ability to perform periodic comparisons of the in-scope biometric records retained in the IDENT system with the in-scope biometric records contained in IAFIS.
STRQ956: IAFIS shall be able to support different populations of data with searches possible against the different populations.
STRQ774: IAFIS shall support the creation of Special Latent Cognizant (SLC) Files.
STRQ944: IAFIS shall be able to support different populations of data with searches possible against the different populations.
STRQ947: IAFIS shall provide a set of segregated sectors of data that can be separately searched using different criteria. Additional sets can be easily added or defined in the future.
STRQ955: IAFIS shall be able to support different populations of data with searches possible against the different populations.
STRQ963: IAFIS shall be able to support different populations of data with searches possible against the different populations.
STRQ957: IAFIS shall be able to support different populations of data with searches possible against the different populations.
STRQ737: IAFIS shall establish multiple logical files, compartmentalizing data in FBI files. Examples of these files are criminal files of: wanted persons, KST, military detainees, undercover agents, witness relocation program, FBI employees, sexual offenders, etc

STRQ944: IAFIS shall be able to support different populations of data with searches possible against the different populations.
STRQ947: IAFIS shall provide a set of segregated sectors of data that can be separately searched using different criteria. Additional sets can be easily added or defined in the future.

STRQ955: IAFIS shall be able to support different populations of data with searches possible against the different populations.
STRQ963: IAFIS shall be able to support different populations of data with searches possible against the different populations.

SFR1543: NGI shall provide the capability to perform intra-repository searches to identify potential Identity consolidations.

BIO.FEAT163: The solution shall provide the capability to search all biometrics in the solution prior to enrollment of a new subject.

BIO.FEAT337: The solution shall include the ability to perform periodic comparisons of the in-scope biometric records retained in the IDENT system with the in-scope biometric records contained in IAFIS.

STRQ956: IAFIS shall be able to support different populations of data with searches possible against the different populations.

STRQ774: IAFIS shall support the creation of Special Latent Cognizant (SLC) Files.

STRQ944: IAFIS shall be able to support different populations of data with searches possible against the different populations.

STRQ947: IAFIS shall provide a set of segregated sectors of data that can be separately searched using different criteria. Additional sets can be easily added or defined in the future.

STRQ955: IAFIS shall be able to support different populations of data with searches possible against the different populations.

STRQ963: IAFIS shall be able to support different populations of data with searches possible against the different populations.

STRQ957: IAFIS shall be able to support different populations of data with searches possible against the different populations.

STRQ737: IAFIS shall establish multiple logical files, compartmentalizing data in FBI files. Examples of these files are criminal files of: wanted persons, KST, military detainees, undercover agents, witness relocation program, FBI employees, sexual offenders, etc

STRQ944: IAFIS shall be able to support different populations of data with searches possible against the different populations.

STRQ947: IAFIS shall provide a set of segregated sectors of data that can be separately searched using different criteria. Additional sets can be easily added or defined in the future.

STRQ955: IAFIS shall be able to support different populations of data with searches possible against the different populations.

STRQ963: IAFIS shall be able to support different populations of data with searches possible against the different populations.

SFR1544: NGI shall provide the capability to perform comparisons of the fingerprint records contained in an External System (e.g., IDENT) with the fingerprint records contained in a specified NGI repository.

SFR1545: NGI shall associate photos with an event if submitted with information identifying a specific event.

STRQ161: The system shall provide the ability to add mug shot photos to the disposition records.

STRQ234: IPS shall allow the ability to associate a photo to a specific arrest, but not be required to send them together.

SFR1546: NGI shall associate photos with the Identity record when submitted without information identifying a specific event.

STRQ467: The system shall update the appropriate records in the IPS using only the submitted FNU.

STRQ1158: The IAFIS IPS shall process a new TOT that supports the submission of images using Type-10 records with an FNU and ten or fewer fingerprint images for identity verification. The photo date field shall be optional. The system shall update the appropriate records in the IPS using only the submitted FNU. If the photo date field was supplied, then a photo message of ?DATE PHOTO TAKEN? shall be appended to the photo. If the date was not supplied, then the date the record was submitted shall be used with the message ?DATE PHOTO SUBMITTED?.

STRQ480: IAFIS shall associate civil photos directly with the civil subject record.

STRQ695: IAFIS shall provide a one-to-one relationship between civil fingerprints and photos.

STRQ1161: The IAFIS IPS shall process Civil TOTs for submission of photos (FANC, FAUF, NFUF, MAP, FNCC, FUFC, MAPC, NFFC, and NFDP). Photos shall be retained if requested, and attached to the civil record using the Civil Record Number.

SFR1547: NGI shall associate photos with the Identity record when the event related to the photos is deleted.

SFR1548: NGI shall associate palmprints with an event if submitted with information identifying a specific event.

SFR1549: NGI shall associate palmprints with the Identity record when submitted without information identifying a specific event.

SFR1550: NGI shall associate palmprints with the Identity record when the event related to the palmprints is deleted.

- SFR1551:** NGI shall associate supplemental fingerprint and palmprint information with an event if submitted with information identifying a specific event.
- SFR1552:** NGI shall associate supplemental fingerprint and palmprint information with the Identity record when submitted without information identifying a specific event.
- SFR1553:** NGI shall associate supplemental fingerprint and palmprint information with the Identity record when the event related to the Supplemental Fingerprint and Palmprint is deleted.
- SFR1554:** NGI shall associate iris information with an event if submitted with information identifying a specific event.
- SFR1555:** NGI shall associate iris information with the Identity when submitted without information identifying a specific event.
- SFR1556:** NGI shall associate iris information with the Identity when the event related to the iris information is deleted.
- SFR1557:** NGI shall retrieve the requested biographic information from the designated repository(ies) for the specified criteria and Identity.
- STRQ265: IAFIS shall provide the option to select the database to search, including the Criminal, Civil, SLC, and ETIS files in a single submission.
- STRQ263: IAFIS shall provide the option to select the database to search, including the Criminal, Civil, SLC, and ETIS files in a single submission.
- STRQ269: IAFIS shall provide the capability to specify the appropriate search criteria for each file in a single submission.
- STRQ267: IAFIS shall provide the capability to specify the appropriate search criteria for each file in a single submission.
- STRQ786: IAFIS shall provide the ability to run/query distinctive parts of the database.
- STRQ784: IAFIS shall provide the ability to run/query distinctive parts of the database.
- SFR1558:** NGI shall retrieve the requested biographic compilation for the specified criteria and Identity.
- STRQ265: IAFIS shall provide the option to select the database to search, including the Criminal, Civil, SLC, and ETIS files in a single submission.
- STRQ263: IAFIS shall provide the option to select the database to search, including the Criminal, Civil, SLC, and ETIS files in a single submission.
- STRQ269: IAFIS shall provide the capability to specify the appropriate search criteria for each file in a single submission.
- STRQ267: IAFIS shall provide the capability to specify the appropriate search criteria for each file in a single submission.
- STRQ786: IAFIS shall provide the ability to run/query distinctive parts of the database.
- STRQ784: IAFIS shall provide the ability to run/query distinctive parts of the database.
- SFR1559:** NGI shall retrieve the requested event Identity information from the designated repository(ies) for the specified criteria and Identity.
- STRQ265: IAFIS shall provide the option to select the database to search, including the Criminal, Civil, SLC, and ETIS files in a single submission.
- STRQ263: IAFIS shall provide the option to select the database to search, including the Criminal, Civil, SLC, and ETIS files in a single submission.
- STRQ269: IAFIS shall provide the capability to specify the appropriate search criteria for each file in a single submission.
- STRQ267: IAFIS shall provide the capability to specify the appropriate search criteria for each file in a single submission.
- STRQ786: IAFIS shall provide the ability to run/query distinctive parts of the database.
- STRQ784: IAFIS shall provide the ability to run/query distinctive parts of the database.
- SFR1560:** NGI shall retrieve the requested biometric information from the designated repository(ies) for the specified criteria and Identity.
- STRQ265: IAFIS shall provide the option to select the database to search, including the Criminal, Civil, SLC, and ETIS files in a single submission.
- STRQ263: IAFIS shall provide the option to select the database to search, including the Criminal, Civil, SLC, and ETIS files in a single submission.
- STRQ269: IAFIS shall provide the capability to specify the appropriate search criteria for each file in a single submission.
- STRQ267: IAFIS shall provide the capability to specify the appropriate search criteria for each file in a single submission.
- STRQ786: IAFIS shall provide the ability to run/query distinctive parts of the database.

STRQ784: IAFIS shall provide the ability to run/query distinctive parts of the database.

SFR1561: NGI shall retrieve the requested composite biometric information for the specified criteria and Identity.

STRQ265: IAFIS shall provide the option to select the database to search, including the Criminal, Civil, SLC, and ETIS files in a single submission.

STRQ263: IAFIS shall provide the option to select the database to search, including the Criminal, Civil, SLC, and ETIS files in a single submission.

STRQ269: IAFIS shall provide the capability to specify the appropriate search criteria for each file in a single submission.

STRQ267: IAFIS shall provide the capability to specify the appropriate search criteria for each file in a single submission.

STRQ786: IAFIS shall provide the ability to run/query distinctive parts of the database.

STRQ784: IAFIS shall provide the ability to run/query distinctive parts of the database.

SFR1562: NGI shall enroll an Identity as a result of a direct biometric enrollment request.

SFR1563: NGI shall create a unique UCN for the Identity as part of an Identity enrollment.

BIO.FEAT370: The solution shall provide an unique identifier other than the FNU for each fingerprint image shared.

BIO.FEAT371: The solution shall exclude the FNU for each fingerprint image shared.

BIO.FEAT373: The solution shall provide the capability to access Criminal History Record Information based on the unique identifier provided for shared fingerprint images.

STRQ512: The IAFIS civil and criminal repositories after redesign and consolidation shall be completely interoperable.

STRQ511: The IAFIS civil and criminal repositories (fingerprint image, fingerprint vector, and biographical data) after redesign and consolidation shall be completely interoperable, implementing single subject identity and providing a full range of capabilities needed to maintain them.

SFR1564: NGI shall determine a unique event identifier for the Identity and Event as part of an Identity enrollment.

BIO.FEAT370: The solution shall provide an unique identifier other than the FNU for each fingerprint image shared.

BIO.FEAT371: The solution shall exclude the FNU for each fingerprint image shared.

BIO.FEAT373: The solution shall provide the capability to access Criminal History Record Information based on the unique identifier provided for shared fingerprint images.

SFR1565: NGI shall enroll biographic information into the designated repository(ies) as part of an Identity enrollment.

STRQ105: IAFIS shall be able to store state-captured origin of persons identification information on a type 2 record, i.e. driver's license, state ID, etc.

STRQ240: IAFIS shall expand the name field (Element ID "NAM", EFTS Tag 2.018 and 2.064B) from 30 characters to 50-60 to accommodate longer names.

SFR1566: NGI shall associate the enrolled biographic information with the unique event identifier as part of an Identity enrollment.

SFR1567: NGI shall associate the enrolled biometric information with the unique event identifier as part of an Identity enrollment.

SFR1568: NGI shall enroll event information into the designated repository(ies) as part of an Identity enrollment.

STRQ154: IAFIS shall store a charge classification that indicates if the arrest charge is a felony or misdemeanor.

SFR1569: NGI shall associate the enrolled event information with the unique event identifier as part of an Identity enrollment.

SFR1570: NGI shall create a biographic compilation as part of an Identity enrollment.

SFR1571: NGI shall associate the biographic compilation with the unique Identity as part of an Identity enrollment.

SFR1572: NGI shall create biometric composite(s) in accordance with biometric file maintenance business rules as part of an Identity enrollment.

STRQ527: The NPPS shall populate a new palm print repository (PPR).

STRQ1163: The NPPS shall allow the capture, storage, and searching of palm prints from a Federal data repository in supporting Federal and State law enforcement agencies. The NPPS shall be a fully automated segment within IAFIS. The NPPS shall accept electronically submitted palm print images in accordance with ANSI/NIST standards and future Electronic Fingerprint Transmission Specification (EFTS) revisions. The NPPS shall have a Standard Palm Print Enrollment (SPPE) in which a contributor submits a palm print image at the same time the contributor submits a ten-print image. The NPPS shall populate a new Palm Print Repository (PPR), and also develop a Bulk Palm Print Enrollment (BPPE).

SFR1573: NGI shall associate the biometric composite with the unique Identity as part of an Identity enrollment.

SFR1574: NGI shall create an Event certification copy containing all the original Identity data for a specific event as part of an Identity enrollment.

SFR1575: NGI shall determine a unique event identifier for the Identity and Event as part of an Identity update.

SFR1576: NGI shall enroll biographic information into the designated repository(ies) as part of an Identity update.

STRQ105: IAFIS shall be able to store state-captured origin of persons identification information on a type 2 record, i.e. driver's license, state ID, etc.

STRQ240: IAFIS shall expand the name field (Element ID "NAM", EFTS Tag 2.018 and 2.064B) from 30 characters to 50-60 to accommodate longer names.

SFR1577: NGI shall associate biographic information with the unique event identifier as part of an Identity update.

SFR1578: NGI shall associate biometric information with the unique event identifier as part of an Identity update.

SFR1579: NGI shall enroll event information into the designated repository(ies) as part of an Identity update.

STRQ154: IAFIS shall store a charge classification that indicates if the arrest charge is a felony or misdemeanor.

SFR1580: NGI shall associate event information with the unique event identifier as part of an Identity update.

SFR1581: NGI shall update the biographic compilation, if applicable, for the Identity as part of an Identity update.

BIO.FEAT304: The solution shall update retained records automatically when subject information is added.

BIO.FEAT305: The solution shall update retained records automatically when subject information is updated.

BIO.FEAT306: The solution shall update retained records automatically when subject information is deleted.

STRQ240: IAFIS shall expand the name field (Element ID "NAM", EFTS Tag 2.018 and 2.064B) from 30 characters to 50-60 to accommodate longer names.

SFR1582: NGI shall create a biometric composite(s) in accordance with biometric file maintenance business rules as part of an Identity update.

BIO.FEAT190: The solution shall maintain or improve the image quality of a print once captured after a confirmed biometric identification.

SFR1583: NGI shall associate the biometric composite(s) with the unique Identity as part of an Identity update.

SFR1584: NGI shall update the biometric composite(s) for the Identity in accordance with biometric file maintenance business rules as part of an Identity update.

BIO.FEAT190: The solution shall maintain or improve the image quality of a print once captured after a confirmed biometric identification.

BIO.FEAT304: The solution shall update retained records automatically when subject information is added.

BIO.FEAT305: The solution shall update retained records automatically when subject information is updated.

BIO.FEAT306: The solution shall update retained records automatically when subject information is deleted.

STRQ279: IAFIS shall maintain a composite set of palm prints.

STRQ527: The NPPS shall populate a new palm print repository (PPR).

STRQ1163: The NPPS shall allow the capture, storage, and searching of palm prints from a Federal data repository in supporting Federal and State law enforcement agencies. The NPPS shall be a fully automated segment within IAFIS. The NPPS shall accept electronically submitted palm print images in accordance with ANSI/NIST standards and future Electronic Fingerprint Transmission Specification (EFTS) revisions. The NPPS shall have a Standard Palm Print Enrollment (SPPE) in which a contributor submits a palm print image at the same time the contributor submits a ten-print image. The NPPS shall populate a new Palm Print Repository (PPR), and also develop a Bulk Palm Print Enrollment (BPPE).

STRQ534: The NPPS, upon submission of a palm print, shall create a Palm Print Repository Record (PPRR).

STRQ1164: The NPPS shall provide a system to internal and external customers with the capability to search both known and unknown candidate repositories, generate queries, create linkages, and perform searches of CJIS Systems of Services (SoS) data in support of criminal investigations. The NPPS shall provide enrollment and identification capabilities similar to what is currently available via ten-print. The NPPS, upon submission of a palm print, shall create a Palm Print Repository Record (PPRR).

SUR13: NGI shall enroll palmprints as part of a Tenprint Fingerprint Identification Search.

SFR732: NGI shall forward a response from an External System (e.g., IDENT) to the Authorized Contributor, independent from the NGI response, as a result of an External Latent Print Feature Investigation Search request.

SUR67: NGI shall support Latent Investigation Searches of an external biometric repository.

BIO.FEAT179: The solution shall identify records as latent prints.

SUR70: NGI shall support Latent Print Image Investigation Searches.

LEG.UR20: IAFIS shall provide a candidate list in response to a Latent Image Search Request.

STRQ82: The IAFIS transaction for latent palm print searches shall be able to expand the number of candidates for high priority cases.

STRQ329: NPPS shall allow the number of candidates returned for latent searches for major crimes, or events, to be increased dynamically.

STRQ538: IAFIS shall allow the number of candidates returned by a palm latent search to be user-defined.

STRQ111: Latent palm print services shall be integrated with, and provide the same services, as latent fingerprint services provided currently; applicable hardware, software, training and documentation shall be provided

STRQ110: Latent palm print services shall provide the same services as latent fingerprint services provided currently; applicable hardware, software, training and documentation shall be provided

STRQ226: IAFIS shall allow alternative means to identify individuals without fingerprints, such as badly injured hands or fingers, missing hands or fingers, etc.

STRQ224: IAFIS shall allow alternative means to identify individuals without fingerprints, such as badly injured hands or fingers, missing hands or fingers, etc.

STRQ529: The NPPS shall provide search capabilities of the palm print repository.

- STRQ1163: The NPPS shall allow the capture, storage, and searching of palm prints from a Federal data repository in supporting Federal and State law enforcement agencies. The NPPS shall be a fully automated segment within IAFIS. The NPPS shall accept electronically submitted palm print images in accordance with ANSI/NIST standards and future Electronic Fingerprint Transmission Specification (EFTS) revisions. The NPPS shall have a Standard Palm Print Enrollment (SPPE) in which a contributor submits a palm print image at the same time the contributor submits a ten-print image. The NPPS shall populate a new Palm Print Repository (PPR), and also develop a Bulk Palm Print Enrollment (BPPE).
- STRQ531: The NPPS shall provide a system to internal and external customers with the capability to search both known and unknown candidate repositories, generate queries, create linkages, and perform searches of CJIS System of Services (SoS) data in support of criminal investigations.
- STRQ1164: The NPPS shall provide a system to internal and external customers with the capability to search both known and unknown candidate repositories, generate queries, create linkages, and perform searches of CJIS Systems of Services (SoS) data in support of criminal investigations. The NPPS shall provide enrollment and identification capabilities similar to what is currently available via ten-print. The NPPS, upon submission of a palm print, shall create a Palm Print
- STRQ536: Latent Examiners shall have a Latent Palm Print Search (LPPS) capability to capture images, adjust minutia marker and enter case information.
- STRQ1165: The NPPS shall provide image retrieval for palm print comparisons by latent examiners and services for unsolved latent palm prints. Latent Examiners shall have a Latent Palm Print Search (LPPS) capability to capture images, adjust minutia marker and enter case information.
- STRQ539: NPPS shall provide the ability to search specific areas of a palm print.
- STRQ557: IAFIS shall provide the capability to search Major Case Prints.
- STRQ980: The system shall search palm prints.
- STRQ133: IAFIS shall provide the ability to search palm prints in the IAFIS repositories.
- STRQ284: IAFIS shall provide the capability to search palm prints similar to what is available for ten-print searches.
- STRQ556: IAFIS shall provide the capability to search palm vs. palm.
- STRQ1090: IAFIS shall not require the identification of palm regions to search for palm print submissions
- STRQ5: NPPS shall have the capability to search specific sections of the print.
- STRQ4: NPPS shall have the capability to search specific sections of the print. The Type 14 or 15 records may hold both palm and major case prints.
- STRQ328: NPPS shall provide the ability to search against specific areas of a palm print.

- STRQ637: IAFIS shall allow searches of palm prints by regions.
- STRQ1089: IAFIS shall require identification of palm region to search for palm print submissions for non-major crimes.
- STRQ1102: IAFIS shall provide the ability to search latent palm prints against a list of suspects.
- STRQ1104: IAFIS shall allow palm print submissions for major crimes to have higher priority.
- SUR71: NGI shall support Latent Print Feature Investigation Searches.
- LEG.UR21: IAFIS shall support Latent Feature Search requests of specified repositories.
- LEG.UR22: IAFIS shall provide a candidate list in response to a Latent Feature Search request.
- STRQ82: The IAFIS transaction for latent palm print searches shall be able to expand the number of
- STRQ329: NPPS shall allow the number of candidates returned for latent searches for major crimes, or events, to be increased dynamically.
- STRQ538: IAFIS shall allow the number of candidates returned by a palm latent search to be user-defined.
- STRQ111: Latent palm print services shall be integrated with, and provide the same services, as latent fingerprint services provided currently; applicable hardware, software, training and documentation shall be provided
- STRQ110: Latent palm print services shall provide the same services as latent fingerprint services provided currently; applicable hardware, software, training and documentation shall be provided
- STRQ226: IAFIS shall allow alternative means to identify individuals without fingerprints, such as badly injured hands or fingers, missing hands or fingers, etc.
- STRQ224: IAFIS shall allow alternative means to identify individuals without fingerprints, such as badly injured hands or fingers, missing hands or fingers, etc.
- STRQ529: The NPPS shall provide search capabilities of the palm print repository.
- STRQ1163: The NPPS shall allow the capture, storage, and searching of palm prints from a Federal data repository in supporting Federal and State law enforcement agencies. The NPPS shall be a fully automated segment within IAFIS. The NPPS shall accept electronically submitted palm print images in accordance with ANSI/NIST standards and future Electronic Fingerprint Transmission Specification (EFTS) revisions. The NPPS shall have a Standard Palm Print Enrollment (SPPE) in which a contributor submits a palm print image at the same time the contributor submits a ten-print image. The NPPS shall populate a new Palm Print Repository (PPR), and also develop a Bulk Palm Print Enrollment (BPPE).
- STRQ531: The NPPS shall provide a system to internal and external customers with the capability to search both known and unknown candidate repositories, generate queries, create linkages, and perform searches of CJIS System of Services (SoS) data in support of criminal investigations.

STRQ1164: The NPPS shall provide a system to internal and external customers with the capability to search both known and unknown candidate repositories, generate queries, create linkages, and perform searches of CJIS Systems of Services (SoS) data in support of criminal investigations. The NPPS shall provide enrollment and identification capabilities similar to what is currently available via ten-print. The NPPS, upon submission of a palm print, shall create a Palm Print Repository Record (PPRR).

STRQ536: Latent Examiners shall have a Latent Palm Print Search (LPPS) capability to capture images, adjust minutia marker and enter case information.

STRQ1165: The NPPS shall provide image retrieval for palm print comparisons by latent examiners and services for unsolved latent palm prints. Latent Examiners shall have a Latent Palm Print Search (LPPS) capability to capture images, adjust minutia marker and enter case information.

STRQ539: NPPS shall provide the ability to search specific areas of a palm print.

STRQ557: IAFIS shall provide the capability to search Major Case Prints.

STRQ980: The system shall search palm prints.

STRQ133: IAFIS shall provide the ability to search palm prints in the IAFIS repositories.

STRQ284: IAFIS shall provide the capability to search palm prints similar to what is available for ten-print searches.

STRQ556: IAFIS shall provide the capability to search palm vs. palm.

STRQ1090: IAFIS shall not require the identification of palm regions to search for palm print submissions for major crimes.

STRQ5: NPPS shall have the capability to search specific sections of the print.

STRQ4: NPPS shall have the capability to search specific sections of the print. The Type 14 or 15 records may hold both palm and major case prints.

STRQ328: NPPS shall provide the ability to search against specific areas of a palm print.

STRQ637: IAFIS shall allow searches of palm prints by regions.

STRQ1089: IAFIS shall require identification of palm region to search for palm print submissions for non-major crimes.

STRQ1102: IAFIS shall provide the ability to search latent palm prints against a list of suspects.

STRQ1104: IAFIS shall allow palm print submissions for major crimes to have higher priority.

STRQ3: Major Case Prints shall be Type 14 and 15.

STRQ1091: IAFIS shall require identification of the orientation for palm print submissions for non-major crimes.

STRQ1092: IAFIS shall not require the identification of orientation for palm print submissions for non-major crimes.

SUR1: NGI shall support Tenprint Fingerprint Identification Search requests.

LEG.UR1: IAFIS shall support Tenprint Fingerprint Identification Search requests.

SFR1585: NGI shall create an Event certification copy containing all original identification information for a specific event as part of an Identity update.

SFR1586: NGI shall update biographic information, if applicable, for the Identity as part of a biographic update.

SFR1587: NGI shall update event information, if applicable, for the Identity as part of an event update.

SFR1588: NGI shall delete all biographic information associated with the Identity as part of an Identity deletion.

SFR1589: NGI shall delete all biometric information associated with the Identity as part of an Identity deletion.

SFR1590: NGI shall delete the biographic compilation associated with the Identity as part of an Identity deletion.

SFR1591: NGI shall delete all biometric composite information associated with the Identity as part of an Identity deletion.

SFR1592: NGI shall delete all event information associated with the Identity as part of an Identity deletion.

SFR1593: NGI shall mark the UCN for a deleted Identity as deleted.

SFR1594: NGI shall allow complete restoration of an Identity within a specified period of time following Identity deletion.

SFR1595: NGI shall re-associate the biographic information associated with the Event to the Identity as part of an Event deletion.
STRQ313: The system shall accept, from the owner of a civil record, transactions that request deletion of the record from the civil repository.

SFR1596: NGI shall re-associate the biometric information associated with the Event to the Identity as part of an Event deletion.
STRQ313: The system shall accept, from the owner of a civil record, transactions that request deletion of the record from the civil repository.

SFR1597: NGI shall delete the event information associated with the Event as part of an Event deletion.
STRQ313: The system shall accept, from the owner of a civil record, transactions that request deletion of the record from the civil repository.

SFR1598: NGI shall mark the unique Event identifier as deleted, for the deleted event as part of an Event deletion.

SFR1599: NGI shall delete the specified biometric information as part of a biometric deletion.
STRQ313: The system shall accept, from the owner of a civil record, transactions that request deletion of the record from the civil repository.

SFR1600: NGI shall delete the specified biometric information from the biometric composite in accordance with biometric file maintenance business rules as part of a biometric deletion.
STRQ313: The system shall accept, from the owner of a civil record, transactions that request deletion of the record from the civil repository.

SFR1601: NGI shall update the biometric composite(s) associated with the Identity in accordance with biometric file maintenance business rules as part of a biometric deletion.
SUR145: NGI shall support the maintenance of palmprints.

SFR1602: NGI shall delete the specified biographic information as part of a biographic deletion.
STRQ313: The system shall accept, from the owner of a civil record, transactions that request deletion of the record from the civil repository.

SFR1603: NGI shall delete the specified biographic information from the biographic compilation, if applicable, as part of a biographic deletion.
STRQ313: The system shall accept, from the owner of a civil record, transactions that request deletion of the record from the civil repository.

SFR1604: NGI shall update the biographic compilation associated with the Identity, if applicable, as part of a biographic deletion.

SFR1605: NGI shall comply with the data retention rules for the External System (e.g., IDENT).
BIO.FEAT185: The solution shall adhere to the data retention policies of the data owner.

SFR1606: NGI shall provide the capability to maintain External System data retention rules for fingerprint transactions.
BIO.FEAT185: The solution shall adhere to the data retention policies of the data owner.

SFR1607: NGI shall support the maintenance of external system link identifiers (i.e., FIN) for multiple External Systems.

SFR1608: NGI shall maintain one unique external system link identifier per External System for an Identity.
BIO.FEAT39: The solution shall associate all biographic information captured during previous interactions to the enumerator, FNU, and/or CRN of that individual.
BIO.FEAT43: The solution shall associate biometrically-confirmed criminal information to the enumerator and/or FNU.
BIO.FEAT44: The solution shall associate biometrically-confirmed civil background information to the enumerator and/or CRN.
BIO.FEAT69: The solution shall always associate any updated information (biometrics, biographics, source of biographical information, individual's role, criminal history, civil background history) to the enumerator, FNU, and/or CRN of that individual.

BIO.FEAT163: The solution shall provide the capability to search all biometrics in the solution prior to enrollment of a new subject.

BIO.FEAT273: The solution shall always associate any updated information (biometrics, biographics, source of biographical information, criminal history) to the enumerator and/or FNU of that individual.

SFR1609: NGI shall associate an external system's link identifier with only one Identity.

BIO.FEAT39: The solution shall associate all biographic information captured during previous interactions to the enumerator, FNU, and/or CRN of that individual.

BIO.FEAT43: The solution shall associate biometrically-confirmed criminal information to the enumerator and/or FNU.

BIO.FEAT44: The solution shall associate biometrically-confirmed civil background information to the enumerator and/or CRN.

BIO.FEAT69: The solution shall always associate any updated information (biometrics, biographics, source of biographical information, individual's role, criminal history, civil background history) to the enumerator, FNU, and/or CRN of that individual.

BIO.FEAT163: The solution shall provide the capability to search all biometrics in the solution prior to enrollment of a new subject.

BIO.FEAT273: The solution shall always associate any updated information (biometrics, biographics, source of biographical information, criminal history) to the enumerator and/or FNU of that individual.

SFR1610: NGI shall maintain the external system link identifier and source system.

BIO.FEAT69: The solution shall always associate any updated information (biometrics, biographics, source of biographical information, individual's role, criminal history, civil background history) to the enumerator, FNU, and/or CRN of that individual.

BIO.FEAT273: The solution shall always associate any updated information (biometrics, biographics, source of biographical information, criminal history) to the enumerator and/or FNU of that individual.

SFR1611: NGI shall maintain the CCA File that contains contributor data (e.g., list of addresses) for Authorized Contributors.

LEG.FR436: IAFIS shall maintain the Computerized Contributor File which contains contributor data (e.g., list of addresses) for Authorized Contributors.

SFR1612: NGI shall support the association of discontinued (retired) contributor identifiers to another active contributor record in the NGI CCA File.

LEG.FR437: IAFIS shall support the association of discontinued (retired) Contributor identifiers to another active Contributor records in the IAFIS CCA File.

SFR1613: NGI shall provide electronic responses to Authorized Contributors using contributor data (e.g., e-mail address) contained within NGI CCA File.

LEG.FR438: IAFIS shall provide electronic responses to Authorized Contributors using contributor data (i.e., e-mail address) contained within IAFIS CCA File.

SFR1614: NGI shall provide hardcopy responses to Authorized Contributors using contributor data (e.g., mailing address) contained within NGI CCA File.

LEG.FR439: IAFIS shall generate hardcopy responses to Authorized Contributors using contributor data (i.e., mailing address) contained within IAFIS CCA File.

SFR1615: NGI shall accept an NCIC ORI File Maintenance message in accordance with the III/NFF Operations and Technical Manual.

LEG.FR440: IAFIS shall accept NCIC ORI File Maintenance message in accordance with the III Operation and Technical Manual.

SFR1616: NGI shall update the NCIC ORI File using the data contained within the NCIC ORI File Maintenance message.

LEG.FR441: IAFIS shall update the NCIC ORI File using the data contained within the NCIC ORI File Maintenance message.

SFR1617: NGI shall accept an NCIC Line File Maintenance message in accordance with the III/NFF Operations and Technical Manual.

LEG.FR442: IAFIS shall accept NCIC Line File Maintenance message in accordance with the III Operation and Technical Manual.

SFR1618: NGI shall update the NCIC Line File using the data contained within the NCIC Line File Maintenance message.

LEG.FR443: IAFIS shall update the NCIC Line File using the data contained within the NCIC Line File Maintenance message.

SFR1619: NGI shall provide the capability to maintain photo enrollment MOU information.

SFR1620: NGI shall provide the capability to maintain palmprint enrollment MOU information.

SFR1621: NGI shall provide the capability to maintain supplemental fingerprint and palmprint enrollment MOU information.

- SFR1622:** NGI shall provide the capability to maintain iris enrollment MOU information.
- SFR1623:** NGI shall provide the capability to convert International standard messages into the latest EBTS format.
- SFR1624:** NGI shall provide the capability to convert EBTS standard messages into other International standard formats.
- SFR1625:** NGI shall support multiple categories of fingerprint repositories (i.e., criminal, civil, ULF, SPC Files, RISC).
LEG.FR444: IAFIS shall maintain multiple IAFIS repositories to support the User Services.
- SFR1626:** NGI shall support multiple categories of photo repositories (i.e., criminal, civil, UPF, SPC Files, RISC).
STRQ45: IPS shall provide the capability to build searchable IPS photo files comparable to the latent cognizant files.
STRQ46: IPS shall provide the capability to build searchable IPS photo files comparable to the latent cognizant files.
STRQ50: IPS shall provide the capability to build searchable IPS photo files comparable to the latent cognizant files.
STRQ633: The system shall support the ability to include photos (mug shots and SMTs) in SLC files.
STRQ762: IAFIS shall allow the construction of a special population to hold photos of national security interest with appropriate demographic data and restrict access to a limited set of users.
STRQ765: IAFIS shall have the ability to maintain an "unsolved photo" file.
- SFR1627:** NGI shall support multiple categories of palmprint repositories (i.e., criminal, civil, ULF, SPC Files, RISC).
STRQ364: NPPS shall be fully integrated with the Enhanced Terrorist Information System (ETIS).
STRQ527: The NPPS shall populate a new palm print repository (PPR).
STRQ1163: The NPPS shall allow the capture, storage, and searching of palm prints from a Federal data repository in supporting Federal and State law enforcement agencies. The NPPS shall be a fully automated segment within IAFIS. The NPPS shall accept electronically submitted palm print images in accordance with ANSI/NIST standards and future Electronic Fingerprint Transmission Specification (EFTS) revisions. The NPPS shall have a Standard Palm Print Enrollment (SPPE) in which a contributor submits a palm print image at the same time the contributor submits a ten-print image. The NPPS shall populate a new Palm Print
STRQ1037: IAFIS shall establish an Unsolved Latent File for palm prints that can be searched.
STRQ1036: IAFIS shall establish an Unsolved Latent File for palm prints that can be searched. NPPS shall have the ability to search against Unsolved Latent Palms.
- SFR1628:** NGI shall support multiple categories of supplemental fingerprint and palmprint repositories (i.e., criminal, civil, ULF, SPC Files, RISC).
STRQ364: NPPS shall be fully integrated with the Enhanced Terrorist Information System (ETIS).
- SFR1629:** Deleted.
- SFR1630:** NGI shall support multiple categories of iris repositories (i.e., criminal, civil, UIF, SPC Files, RISC).
- SFR1631:** NGI shall provide the capability to populate the RISC with information from external repositories.
BIO.FEAT25: The solution shall be able to accept biographic and biometric information from external biometric systems.
- SFR1632:** NGI shall maintain unique external repository identifiers for RISC records that are populated by external repositories.
- SFR1633:** NGI shall maintain the ITF as a subset of records within the RISC repository.
- SFR1634:** NGI shall provide the capability to synchronize the RISC with information from other repositories (internal or external).
- SFR1635:** NGI shall write selected information contained in NGI repository(ies) to media (e.g., CD, DVD) as part of a bulk media export request.
LEG.FR445: IAFIS shall write selected information contained in IAFIS repository(s) to media (e.g. CD, DVD, etc.) as part of a bulk media export request.
- SFR1636:** NGI shall provide an automated capability for an Authorized FBI System Administrators to bulk export event certification copies.
STRQ216: IAFIS shall provide the capability of downloading master fingerprint images from IAFIS in bulk.
- SFR1637:** NGI shall allow an Authorized FBI System Administrator to select information from the designated NGI repository(ies) as part of a bulk media export request.
STRQ217: IAFIS shall provide the capability of writing master fingerprint images from IAFIS in bulk to a CD or DVD.

- SFR1639: NGI shall support removable media for bulk import of fingerprint information.**
- SFR1640: NGI shall accept bulk enrollment requests for the ITF via multiple methods (e.g., ftp, CD, DVD).**
- SFR1641: NGI shall maintain a repository maintenance transaction log for each repository.**
LEG.FR446: IAFIS shall maintain a repository maintenance transaction log for each repository.
- SFR1642: NGI shall create an entry in the repository maintenance transaction log for each creation, deletion and update action.**
LEG.FR447: IAFIS shall create an entry in the repository maintenance transaction log pertaining to record creation/deletion/update actions for each.
- SFR1643: NGI shall support the use of the repository maintenance transaction log to restore the repository to a point in time.**
LEG.FR448: IAFIS shall support the use of the repository maintenance transaction log to restore the repository to a point in time in the past.
- SFR1644: NGI shall allow Authorized System Security Administrators to terminate any or all transactions and processes occurring in any environment independent of other NGI environments.**
LEG.FR449: IAFIS shall allow authorized System Security Administrators to terminate any or all transactions and processes occurring in any environment independent of other IAFIS environments.
- SFR1645: NGI shall allow Authorized System Administrators to terminate any or all transactions and processes occurring in any environment independent of other NGI environments.**
LEG.FR450: IAFIS shall allow authorized System Administrators to terminate any or all transactions and processes occurring in any environment independent of other IAFIS environments.
- SFR1646: NGI shall support centralized control and display of system administration functions.**
LEG.FR451: IAFIS shall support centralized control and display of system administration functions.
- SFR1647: NGI shall support centralized control and display of system security administration functions.**
LEG.FR452: IAFIS shall support centralized control and display of system security administration functions.
- SFR1648: NGI shall report system alarms to a centralized system administration display.**
LEG.FR453: IAFIS shall report system alarms to centralized system administration display.
- SFR1649: NGI shall support an Authorized System Administrator initiating diagnostic testing of NGI or identified systems/functions.**
LEG.FR454: IAFIS shall support an Authorized System Administrator initiating diagnostic testing of IAFIS or identified systems/functions.
- SFR1650: NGI shall support an Authorized System Administrator initiating and controlling system data backup and restore functions.**
LEG.FR455: IAFIS shall support an Authorized System Administrator initiating and controlling system data backup and restore functions.
- SFR1651: NGI shall support an Authorized System Administrator initiating the start command for each component of the NGI system allowing for the orderly start of NGI operations.**
LEG.FR456: IAFIS shall support an Authorized System Administrator initiating start command for each component IAFIS system allowing for the orderly start of IAFIS operations.
- SFR1652: NGI shall support an Authorized System Administrator initiating a shutdown command for each component of the NGI system allowing for the orderly shut down of NGI operations.**
LEG.FR457: IAFIS shall support an Authorized System Administrator initiating shutdown command for each component of IAFIS system allowing for the orderly shut down of IAFIS operations.
- SFR1653: NGI shall support an Authorized System Administrator reallocating resources to level the processing workload.**
LEG.FR458: IAFIS shall support an Authorized System Administrator reallocating of resources to level the processing workload.
- SFR1654: NGI shall support an Authorized System Administrator changing transaction processing priorities.**
LEG.FR459: IAFIS shall support an Authorized System Administrator changing transaction processing priorities.
- SFR1655: NGI shall provide an Authorized System Administrator with the capability to cancel a transaction being processed, suspend a transaction, and redirect processing to another work queue.**

LEG.FR460: IAFIS shall provide an Authorized System Administrator with the ability to cancel a transaction being processed, suspend a transaction, and redirect processing to another work queue.

SFR1656: NGI shall allow an Authorized System Administrator to create a new NGI repository with no impact to NGI User Services.

SFR1657: NGI shall allow an Authorized System Administrator to create access rules for a new NGI repository.

SFR1658: NGI shall allow an Authorized System Administrator to create enrollment rules for a new NGI repository.

SFR1659: NGI shall allow an Authorized System Administrator to create dissemination rules for a new NGI repository.

SFR1660: NGI shall provide an extensible workflow management capability.

LEG.FR461: IAFIS shall provide a workflow management capability.

SFR1661: NGI shall support the integration of new biometrics into the workflow management functions without negatively impacting existing NGI workflow.

SFR1662: NGI shall manage the processing of each transaction based on the transaction type and transaction processing rules.

LEG.FR462: IAFIS shall manage the processing of each transaction based on the transaction type and transaction processing rules.

SFR1663: NGI shall assign tasks to a work queue consistent with transaction processing rules.

LEG.FR463: IAFIS shall assign tasks to a work queue consistent with transaction processing rules.

SFR1664: NGI shall allow an Authorized System Administrator the capability to adjust the rate of transactions input into NGI.

LEG.FR464: IAFIS shall allow an Authorized System Administrator the ability to adjust the rate of transactions input into IAFIS.

SFR1665: NGI shall collect data and statistics needed to support the management of work queues.

LEG.FR465: IAFIS shall collect data and statistics needed to support the management of work queues.

SFR1666: NGI shall support the creation of backup data for NGI repository data.

LEG.FR466: IAFIS shall support the creation of backup data for IAFIS repository data.

SFR1667: NGI shall support the creation of backup data for NGI system files.

LEG.FR467: IAFIS shall support the creation of backup data for IAFIS system files.

SFR1668: NGI shall support the creation of backup data for NGI application files.

LEG.FR468: IAFIS shall support the creation of backup data for IAFIS application files.

SFR1669: NGI shall support the recovery of NGI repository data from backup files.

LEG.FR469: IAFIS shall support the recovery of IAFIS repository data from backup files.

SFR1670: NGI shall support the recovery of NGI system files from backup files.

LEG.FR470: IAFIS shall support the recovery of IAFIS system files from backup files.

SFR1671: NGI shall support the recovery of NGI application files from backup files.

LEG.FR471: IAFIS shall support the recovery of IAFIS application files from backup files.

SFR1672: NGI shall provide core NGI services during backup operations.

LEG.FR472: IAFIS shall ensure that core IAFIS services are available during backup operations.

SFR1673: NGI shall support export of backup data to removable media.

LEG.FR473: IAFIS shall support export of backup data to removable media.

SFR1674: NGI shall support an interface to NCIC in accordance with the III/NFF Operations and Technical Manual.

LEG.FR474: IAFIS shall support an interface to NCIC in accordance with the III Operation and Technical Manual.

SFR1675: NGI shall support an interface to Nlets in accordance with the Nlets Users Guide.

BIO.FEAT403: The notification delivered to the LESC shall follow Nlets User and Technical Guidelines.

LEG.FR475: IAFIS shall support an interface to Nlets in accordance with the Nlets Users Guide.

SFR1676: NGI shall support an interface to the CJIS WAN in accordance with the latest EBTS version.

LEG.FR527: IAFIS shall support an interface to the CJIS WAN in accordance with the latest EBTS version.

SFR1677: NGI shall support an Internet interface for all NGI User Services.

STRQ69: The NPPS shall have the capability to utilize web services.

STRQ67: The NPPS shall allow bulk submission of palm prints using web services.

STRQ87: IAFIS shall allow the user to enter more than 10 charges via the Internet, LEO and FTP.

STRQ1169: IAFIS shall allow the user to enter more than 10 charges.

STRQ257: LPW shall be modified to allow remote search to IAFIS using a PC based solution.

STRQ256: LPW shall be modified to allow remote search and submission to IAFIS using a PC based solution.

STRQ258: LPW shall be modified to allow remote submission to IAFIS using a PC based solution.

STRQ256: LPW shall be modified to allow remote search and submission to IAFIS using a PC based solution.

STRQ272: FBI LPW shall allow remote access to the IAFIS Civil Files

STRQ502: The Machine Readable Data (MRD) process shall be modernized to make use of the Internet.

STRQ501: The Machine Readable Data (MRD) process shall be modernized to make use of the Internet, Law Enforcement Online (LEO) network and compact disc read-only (CD-ROM) formatting.

STRQ508: IAFIS shall accept bulk dispositions submitted through the Internet.

STRQ606: IAFIS shall provide more connectivity options so that sending latent prints and receiving results to the FBI crime lab from Interpol is possible.

SFR1678: NGI shall support a LEO interface for all NGI User Services.

STRQ87: IAFIS shall allow the user to enter more than 10 charges via the Internet, LEO and FTP.

STRQ1169: IAFIS shall allow the user to enter more than 10 charges.

STRQ503: The Machine Readable Data (MRD) process shall be modernized to make use of the Law Enforcement Online (LEO) network.

STRQ501: The Machine Readable Data (MRD) process shall be modernized to make use of the Internet, Law Enforcement Online (LEO) network and compact disc read-only (CD-ROM) formatting.

STRQ509: IAFIS shall accept bulk dispositions submitted through the LEO network.

SFR1679: NGI shall support an enhanced MRD interface for disposition processing.

STRQ87: IAFIS shall allow the user to enter more than 10 charges via the Internet, LEO and FTP.

STRQ1169: IAFIS shall allow the user to enter more than 10 charges.

STRQ169: IAFIS allow the upload of disposition data via FTP.

STRQ342: IAFIS shall support the bulk submissions of dispositions via FTP.

STRQ569: IAFIS shall allow dispositions to be submitted using FTP

STRQ502: The Machine Readable Data (MRD) process shall be modernized to make use of the Internet.

STRQ501: The Machine Readable Data (MRD) process shall be modernized to make use of the Internet, Law Enforcement Online (LEO) network and compact disc read-only (CD-ROM) formatting.

STRQ503: The Machine Readable Data (MRD) process shall be modernized to make use of the Law Enforcement Online (LEO) network.

STRQ501: The Machine Readable Data (MRD) process shall be modernized to make use of the Internet, Law Enforcement Online (LEO) network and compact disc read-only (CD-ROM) formatting.

STRQ504: The Machine Readable Data (MRD) process shall be modernized to make use of the compact disc read-only (CD-ROM) formatting.

STRQ501: The Machine Readable Data (MRD) process shall be modernized to make use of the Internet, Law Enforcement Online (LEO) network and compact disc read-only (CD-ROM) formatting.

STRQ508: IAFIS shall accept bulk dispositions submitted through the Internet.

STRQ509: IAFIS shall accept bulk dispositions submitted through the LEO network.

STRQ626: IAFIS shall provide the capability to send dispositions in a flat file via the CJIS WAN, LEO, and the Internet.

SFR1680: NGI shall support removable media for the bulk enrollment of photos.

SFR1681: NGI shall support removable media for the bulk enrollment of palmprints.

SFR1682: NGI shall support removable media for the bulk enrollment of supplemental fingerprint and palmprint information.

SFR1683: NGI shall support removable media for bulk enrollment of iris information.

SFR1684: NGI shall support removable media for bulk export of event certification copies.

STRQ216: IAFIS shall provide the capability of downloading master fingerprint images from IAFIS in bulk.

SFR1686: NGI shall support an interface to external designated repositories in accordance with the latest EBTS version.

BIO.FEAT129: The solution shall employ biometric standards established by the National Institute of Standards and Technology (NIST), i.e. the ANSI National Standard for Information Systems -- Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information, ANSI/NIST-ITL-1-2007.

BIO.FEAT143: User groups currently accessing IAFIS shall have access to both IAFIS and IDENT data through the solution:

BIO.FEAT146: The solution shall allow a user to select type of search in the submission of the query of IAFIS or IDENT and IAFIS.

BIO.FEAT182: The solution shall employ a standard format for query responses.

BIO.FEAT194: The solution shall support EBTS compliant data exchange.

BIO.FEAT370: The solution shall provide a unique identifier other than the FNU for each fingerprint image shared.

BIO.FEAT371: The solution shall exclude the FNU for each fingerprint image shared.

BIO.FEAT373: The solution shall provide the capability to access Criminal History Record Information based on the unique identifier provided for shared fingerprint images.

BIO.FEAT374: The solution shall provide the capability to access immigration data response information based on the unique identifier provided for shared fingerprint images.

STRQ671: IAFIS shall provide an automated notification to TSC to initiate research in classified systems in order to provide answers when known or suspected terrorist (KST) information is queried.

STRQ903: IAFIS will have an interface to the DoD National Security Interest File.

STRQ901: IAFIS will have an interface to the DoD National Security Interest File.

SFR1687: NGI shall collect communications status information on external system interfaces.

LEG.FR476: IAFIS shall collect communications status information on external system interfaces.

SFR1688: NGI shall report communications status of external system interfaces.

LEG.FR477: IAFIS shall report communications status of external system interfaces.

SFR1689: NGI shall collect communications status information on internal system interfaces.

LEG.FR478: IAFIS shall collect communications status information on internal system interfaces.

SFR1690: NGI shall report communications status of internal system interfaces.

LEG.FR479: IAFIS shall report communications status of internal system interfaces.

SFR1691: NGI shall provide Authorized FBI Service Providers with Palmprint miss analysis tool capabilities.

SFR1692: NGI shall provide Authorized Contributors with palmprint information to support miss analysis tools.

SFR1693: NGI shall provide Authorized FBI Service Providers with fingerprint miss analysis tool capabilities.

STRQ1022: IAFIS shall provide a miss analysis tool for latent users

STRQ429: IAFIS shall include a user missed-analysis tool to help determine the cause of the missed identification.

SFR1694: NGI shall provide Authorized Contributors with fingerprint information to support miss analysis tools.

STRQ1022: IAFIS shall provide a miss analysis tool for latent users

STRQ429: IAFIS shall include a user missed-analysis tool to help determine the cause of the missed identification.

SFR1695: NGI shall provide Authorized FBI Service Providers with latent miss analysis tool capabilities.

STRQ1022: IAFIS shall provide a miss analysis tool for latent users

STRQ429: IAFIS shall include a user missed-analysis tool to help determine the cause of the missed identification.

SFR1696: NGI shall provide Authorized Contributors with latent information to support miss analysis tools.

STRQ1022: IAFIS shall provide a miss analysis tool for latent users

STRQ429: IAFIS shall include a user missed-analysis tool to help determine the cause of the missed identification.

SFR1697: NGI shall provide Authorized System Administrators with Subject Search miss analysis tool capabilities.

LEG.FR505: IAFIS shall provide authorized FBI System Administrators with Subject Search miss analysis tool capabilities.

SFR1698: NGI shall collect transaction data for all transactions.

BIO.FEAT106: The solution shall provide agency-to-agency audit trails for data receipt, maintenance, storage, dissemination, and use of shared data.

BIO.FEAT107: The solution shall provide an audit trail of all data capture and update transactions.

BIO.FEAT280: The solution shall create an Activity Log of demoted records.

LEG.FR480: IAFIS shall collect transaction data for all transactions.

SFR1699: NGI shall collect the processing history of all transactions.

BIO.FEAT106: The solution shall provide agency-to-agency audit trails for data receipt, maintenance, storage, dissemination, and use of shared data.

BIO.FEAT107: The solution shall provide an audit trail of all data capture and update transactions.

BIO.FEAT151: The solution shall maintain information on the reason a record change is made.

BIO.FEAT268: The solution shall provide audit details of transaction history including the following: a. Unique Identifier b. Date Processed c. Time Processed

BIO.FEAT280: The solution shall create an Activity Log of demoted records.

STRQ879: IAFIS shall ensure that the disposition submission, along with the information about that submission (source, data, media, format, etc.) should be retained as part of the official record.

STRQ880: IAFIS shall ensure that any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

SFR1700: NGI shall allow an Authorized FBI Service Provider access to transaction history data.

LEG.FR481: IAFIS shall allow Authorized FBI Service Provider access to transaction history data.

SFR1701: NGI shall allow an Authorized FBI Service Provider to view transaction history data.

LEG.FR482: IAFIS shall allow Authorized FBI Service Provider to view transaction history data.

SFR1702: NGI shall allow an Authorized FBI Service Provider to print transaction history data.

LEG.FR483: IAFIS shall allow Authorized FBI Service Provider to print transaction history data.

SFR1703: NGI shall provide a centralized transaction history reporting service.

BIO.FEAT106: The solution shall provide agency-to-agency audit trails for data receipt, maintenance, storage, dissemination, and use of shared data.

BIO.FEAT107: The solution shall provide an audit trail of all data capture and update transactions.

BIO.FEAT151: The solution shall maintain information on the reason a record change is made.

BIO.FEAT268: The solution shall provide audit details of transaction history including the following: a. Unique Identifier b. Date Processed c. Time Processed

BIO.FEAT269: The solution shall provide an audit record of individuals that perform actions in the system.

BIO.FEAT270: The solution shall provide an audit record of the actions that individuals perform in the system.

BIO.FEAT271: The solution shall provide an audit record of the actions performed by the system.

BIO.FEAT280: The solution shall create an Activity Log of demoted records.

BIO.FEAT345: The solution shall provide the ability to report on the query time of the IAFIS query requests.
STRQ932: IAFIS shall provide the ability for CJIS personnel to check the status of the systems.

SFR1704: NGI shall allow an Authorized FBI Service Provider access to a centralized transaction history reporting service.
STRQ932: IAFIS shall provide the ability for CJIS personnel to check the status of the systems.

SFR1705: NGI shall provide the capability to generate statistical reports based on transaction history data.
LEG.FR484: IAFIS shall provide the capability to generate statistical reports based on transaction history data.

SFR1706: NGI shall retain transaction history data.
LEG.FR485: IAFIS shall retain transaction history data.

SFR1707: NGI shall provide parameter-based transaction history reporting capabilities.
BIO.FEAT345: The solution shall provide the ability to report on the query time of the IAFIS query requests.

SFR1708: NGI shall provide pre-defined transaction history reporting capabilities.
BIO.FEAT345: The solution shall provide the ability to report on the query time of the IAFIS query requests.

SFR1709: NGI shall record the quality of fingerprints received as part of fingerprint transactions.
BIO.FEAT98: The solution shall provide the ability to report on the quality of fingerprints captured during any interaction.

SFR1710: NGI shall record into a RISC audit log the dissemination of all RISC information.

SFR1711: NGI shall record the Fingerprint Investigation Search request information to support a fingerprint miss analysis tool.

SFR1712: NGI shall record the Latent Investigation Search request information to support a latent miss analysis tool.

SFR1713: Deleted.

SFR1714: NGI shall record Subject Search request information to support a Subject Search miss analysis tool.
LEG.FR506: IAFIS shall record Subject Search request information to support a Subject Search Miss Analysis Tool.

SFR1715: NGI shall allow an Authorized FBI Service Provider the capability to view the RISC audit log.

SFR1716: NGI shall record into an ITF audit log the dissemination of all ITF information.

SFR1717: NGI shall allow an Authorized FBI Service Provider the capability to print the RISC audit log.

SFR1718: NGI shall record into a fingerprint audit log the dissemination of all fingerprint information.

SFR1719: NGI shall record into an unsolved latent audit log the dissemination of all unsolved latent information.

SFR1720: NGI shall record statute maintenance requests in a statute maintenance audit log.

SFR1721: NGI shall record into a photo audit log the dissemination of all photos.
STRQ690: IAFIS shall provide an audit trail for all photo disseminations.
STRQ1166: IAFIS shall provide an audit trail for all photo inquiries and disseminations.

SFR1722: NGI shall record into a palmprint audit log the dissemination of all palmprints.

SFR1723: NGI shall record into a supplemental fingerprint and palmprint audit log the dissemination of all supplemental fingerprint and palmprint information.

SFR1724: NGI shall record in an iris audit log the dissemination of all iris information
STRQ880: IAFIS shall ensure that any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

SFR1725: NGI shall support fingerprint statistical reporting.
BIO.FEAT102: The solution shall provide the ability to report on the response time for biometric queries.

SFR1726: NGI shall support RISC statistical reporting.

SFR1727: NGI shall support latent statistical reporting.
BIO.FEAT102: The solution shall provide the ability to report on the response time for biometric queries.
STRQ80: IAFIS shall be able to report the number of positive identifications reported to the IAFIS on latent images.

SFR1728: NGI shall support unsolved latent decision statistical reporting.

BIO.FEAT102: The solution shall provide the ability to report on the response time for biometric queries.

SFR1729: NGI shall support SPC File decision statistical reporting.

STRQ788: IAFIS shall capture and report on the quality of the database based on NIST Fingerprint Image Quality (NFIQ).

SFR1730: Deleted.

SFR1731: NGI shall support photo statistical reporting.

BIO.FEAT102: The solution shall provide the ability to report on the response time for biometric queries.

SFR1732: NGI shall support photo decision statistical reporting.

SFR1733: NGI shall support palmprint statistical reporting.

SFR1734: Deleted.

SFR1735: NGI shall support supplemental fingerprint and palmprint statistical reporting.

SFR1736: Deleted.

SFR1738: NGI shall support Identity statistical reporting.

STRQ365: IAFIS shall provide statistical reporting of the number of requests made, the number of identifications returned, and the ratio of those rates for the state's agencies on a monthly basis.

STRQ792: IAFIS shall implement a statistical service to keep track of metrics.

SFR1739: NGI shall support Rap Back statistical reporting.

STRQ792: IAFIS shall implement a statistical service to keep track of metrics.

SFR1740: NGI shall support iris statistical reporting.

STRQ792: IAFIS shall implement a statistical service to keep track of metrics.

SFR1741: NGI shall support iris decision statistical reporting.

STRQ792: IAFIS shall implement a statistical service to keep track of metrics.

SFR1742: NGI shall provide parameter-based management information reporting capabilities.

BIO.FEAT89: The solution shall provide the ability to report on the number and types of hits against criminal information based on biometrically-confirmed interactions.

BIO.FEAT97: The solution shall provide the ability to report on latent print matches against prints stored in in-scope systems.

BIO.FEAT102: The solution shall provide the ability to report on the response time for biometric queries.

BIO.FEAT104: The solution shall provide the ability to report on the number of external requests for biometric information by agency.

BIO.FEAT108: The solution shall provide the ability to perform ad-hoc reports on all available data for a particular user.

SFR1743: NGI shall provide pre-defined management information reporting capabilities.

BIO.FEAT89: The solution shall provide the ability to report on the number and types of hits against criminal information based on biometrically-confirmed interactions.

BIO.FEAT97: The solution shall provide the ability to report on latent print matches against prints stored in in-scope systems.

BIO.FEAT102: The solution shall provide the ability to report on the response time for biometric queries.

BIO.FEAT104: The solution shall provide the ability to report on the number of external requests for biometric information by agency.

SFR1744: NGI shall support transaction statistical reporting.

BIO.FEAT102: The solution shall provide the ability to report on the response time for biometric queries.

BIO.FEAT104: The solution shall provide the ability to report on the number of external requests for biometric information by agency.

SFR1745: NGI shall support fingerprint image quality statistical reporting of NGI Repositories.

BIO.FEAT98: The solution shall provide the ability to report on the quality of fingerprints captured during any interaction.

BIO.FEAT201: The solution shall provide the ability to report on the quality of fingerprints that are already stored in IDENT/IAFIS.

SFR1746: NGI shall support latent print image quality statistical reporting of NGI Repositories.

BIO.FEAT201: The solution shall provide the ability to report on the quality of fingerprints that are already stored in IDENT/IAFIS.

SFR1747: NGI shall support statistical reporting on external system links contained within NGI repositories.

SFR1748: NGI shall provide the capability to report to an External System (e.g., IDENT) on the biometrically-linked information associated with an Identity.

SFR1749: NGI shall support ITF statistical reporting.

SFR1750: NGI shall support ITF trend analysis reporting.

SFR1751: NGI shall collect user fee history data.

LEG.FR486: IAFIS shall collect user fee history data.

SFR1754: NGI shall calculate user fees for each chargeable transaction based on user fee history data.

LEG.FR487: IAFIS shall calculate user fees for each chargeable IAFIS fingerprint identification processing and name search transaction based on user fee history data.

SFR1755: NGI shall allow Authorized FBI Service Providers access to user fee history, administrative, and billing data.

LEG.FR488: IAFIS shall allow Authorized FBI Service Providers access to user fee history, administrative, and billing data.

SFR1756: NGI shall provide the capability for Authorized FBI Service Providers to maintain (i.e., add, delete, and modify) user fee administrative data.

LEG.FR489: IAFIS shall provide capabilities for Authorized FBI Service Providers to maintain (i.e., add, delete, and modify) user fee administrative data.

STRQ525: The Enhanced IAFIS Repository shall provide civil subject employers and licensing bodies with Rap Back billing services for the notification of new criminal activity.

STRQ520: The Enhanced IAFIS Repository shall notify civil subject employers and licensing bodies of new criminal activity through Rap Back services that include subscription registration and maintenance, status checking, criminal activity detection, response generation, transmission/routing, and billing.

SFR1757: NGI shall provide the capability for Authorized FBI Services Providers to maintain user fee bills.

LEG.FR490: IAFIS shall provide capabilities for Authorized FBI Services Providers to maintain user fee bills.

SFR1758: NGI shall assign a fee for each chargeable transaction.

LEG.FR491: IAFIS shall assign a fee for each chargeable transaction.

STRQ880: IAFIS shall ensure that any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

SFR1759: NGI shall support the generation of user fee bills.

LEG.FR492: IAFIS shall support generation of user fee bills.

STRQ525: The Enhanced IAFIS Repository shall provide civil subject employers and licensing bodies with Rap Back billing services for the notification of new criminal activity.

STRQ520: The Enhanced IAFIS Repository shall notify civil subject employers and licensing bodies of new criminal activity through Rap Back services that include subscription registration and maintenance, status checking, criminal activity detection, response generation,

SFR1760: NGI shall provide the capability to generate hardcopy user fee bills.

LEG.FR493: IAFIS shall provide ability to generate hardcopy user fee bills.

SFR1761: NGI shall provide the capability to generate softcopy user fee bills.

LEG.FR494: IAFIS shall provide ability to generate softcopy user fee bills.

SFR1762: NGI shall support generation of user fee reports.

LEG.FR495: IAFIS shall support generation of user fee reports.

SFR1763: NGI shall retain user fee billing history data.

LEG.FR496: IAFIS shall retain user fee billing history data.

SFR1764: NGI shall retain user fee administrative data.

LEG.FR497: IAFIS shall retain user fee administrative data.

SFR1765: NGI shall provide the capability to regenerate user fee bills.

LEG.FR498: IAFIS shall provide the capability to regenerate user fee bills.

SFR1771: NGI shall support an interface to NCIC in accordance with the NCIC Operating Manual.

LEG.FR528: IAFIS shall support an interface to NCIC in accordance with the NCIC Operating Manual.

SFR1860: NGI shall provide the capability to maintain Rap Back Notification rules.

BIO.FEAT129: The solution shall employ biometric standards established by the National Institute of Standards and Technology (NIST), i.e. the ANSI National Standard for Information Systems -- Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information, ANSI/NIST-ITL-1-2007.

BIO.FEAT182: The solution shall employ a standard format for query responses.

BIO.FEAT194: The solution shall support EBTS compliant data exchange.

STRQ101: The System shall send back all information on the Criminal Justice applicants, retained by the FBI, to Rap Back

STRQ99: The system shall send back all information (criminal history, wanted, suspected terrorists, etc) on Criminal Justice applicants retained by the FBI, for both original request and Rap Back.

STRQ681: IAFIS shall provide electronic Rap Back on all federal employees to OPM and include all biographic identification information.

STRQ897: The system shall route Rap Back notifications electronically back to the submitting non-government channeling institution (e.g., ABA) for distribution to the original subscriber.

SFR1870: NGI shall provide the capability to maintain a daily IAQ search limit.

BIO.FEAT249: When either IDENT or IAFIS stores biometrics that have a biometrically-verified link to information stored within an external system or agency (such as CLAIMS and SEVIS through LESC, DOS CLASS, DOD, and NFF state systems) that interfaces with either IDENT or IAFIS, the solution shall provide access to that information.

LEG.FR645: IAFIS shall provide the capability to maintain a daily IAQ search limit.

SFR1871: NGI shall provide the capability to identify which individual biometric information comprised the biometric composite at any specific time.

STRQ92: IAFIS shall provide all sets of fingerprints for a subject.

STRQ208: IAFIS shall be able to retrieve multiple fingerprint and palm print images for a FBI number.

STRQ207: IAFIS shall be able to retrieve multiple fingerprint and palm print images for a FBI number.

STRQ211: IAFIS shall provide the capability to retrieve multiple fingerprint and palm print images based on the FBI number and DOA.

STRQ210: IAFIS shall provide the capability to retrieve multiple fingerprint and palm print images based on the FBI number and DOA.

STRQ420: IAFIS shall permit an increase in the number of images for each record/finger.

STRQ422: IAFIS shall provide external users with the capability to access the additional fingerprint images (resulting from multiple arrests) that are in the Certification File.

STRQ1023: IAFIS shall allow remote access to the CERT files.

STRQ1100: IAFIS shall retain all fingerprint submissions for use in tenprint and latent searches.

STRQ527: The NPPS shall populate a new palm print repository (PPR).

STRQ1163: The NPPS shall allow the capture, storage, and searching of palm prints from a Federal data repository in supporting Federal and State law enforcement agencies. The NPPS shall be a fully automated segment within IAFIS. The NPPS shall accept electronically submitted palm print images in accordance with ANSI/NIST standards and future Electronic Fingerprint Transmission Specification (EFTS) revisions. The NPPS shall have a Standard Palm Print Enrollment (SPPE) in which a contributor submits a palm print image at the same time the contributor submits a ten-print image. The NPPS shall populate a new Palm Print Repository (PPR), and also develop a Bulk Palm Print Enrollment (BPPE).

SFR1872: NGI shall record, into the biometric composite history log, information indicating which individual biometrics are included in the biometric composite when a biometric composite is created or updated.

STRQ240: IAFIS shall expand the name field (Element ID "NAM", EFTS Tag 2.018 and 2.064B) from 30 characters to 50-60 to accommodate longer names.

STRQ279: IAFIS shall maintain a composite set of palm prints.

STRQ527: The NPPS shall populate a new palm print repository (PPR).

STRQ1163: The NPPS shall allow the capture, storage, and searching of palm prints from a Federal data repository in supporting Federal and State law enforcement agencies. The NPPS shall be a fully automated segment within IAFIS. The NPPS shall accept electronically submitted palm print images in accordance with ANSI/NIST standards and future Electronic Fingerprint Transmission Specification (EFTS) revisions. The NPPS shall have a Standard Palm Print Enrollment (SPPE) in which a contributor submits a palm print image at the same time the contributor submits a ten-print image. The NPPS shall populate a new Palm Print Repository (PPR), and also develop a Bulk Palm Print Enrollment (BPPE).

STRQ534: The NPPS, upon submission of a palm print, shall create a Palm Print Repository Record (PPRR).

STRQ1164: The NPPS shall provide a system to internal and external customers with the capability to search both known and unknown candidate repositories, generate queries, create linkages, and perform searches of CJIS Systems of Services (SoS) data in support of criminal investigations. The NPPS shall provide enrollment and identification capabilities similar to what is currently available via ten-print. The NPPS, upon submission of a palm print, shall create a Palm Print Repository Record (PPRR).

SFR1873: NGI shall provide pre-defined biometric composite history log reporting capabilities

STRQ880: IAFIS shall ensure that any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

STRQ1022: IAFIS shall provide a miss analysis tool for latent users

STRQ429: IAFIS shall include a user missed-analysis tool to help determine the cause of the missed identification.

SFR1874: NGI shall support the control, sequencing, management, input, and output of transactions that are processed as part of the workflow management function.

LEG.FR461: IAFIS shall provide a workflow management capability.

SFR1875: NGI shall provide a project work queue for staging transactions that have no response time requirements.

LEG.FR461: IAFIS shall provide a workflow management capability.

SFR1876: NGI shall allow an Authorized System Administrator to input transactions into the project work queue via multiple methods (e.g. CD, DVD, ftp).

SFR1879: NGI shall provide the capability to maintain business rules to support the ASC function.

SFR1880: NGI shall provide the capability to maintain business rules to support the cascaded searching of NGI repositories.

SFR1881: NGI shall create UCNs that do not indicate chronological order.

STRQ512: The IAFIS civil and criminal repositories after redesign and consolidation shall be completely interoperable.

STRQ511: The IAFIS civil and criminal repositories (fingerprint image, fingerprint vector, and biographical data) after redesign and consolidation shall be completely interoperable, implementing single subject identity and providing a full range of capabilities needed to maintain them.

SFR1882: NCI shall create UCNs that do not indicate repository association.

STRQ512: The IAFIS civil and criminal repositories after redesign and consolidation shall be completely interoperable.

STRQ511: The IAFIS civil and criminal repositories (fingerprint image, fingerprint vector, and biographical data) after redesign and consolidation shall be completely interoperable, implementing single subject identity and providing a full range of capabilities needed to maintain them.

SFR1883: NCI shall create UCNs that contain a built-in redundancy check.

STRQ512: The IAFIS civil and criminal repositories after redesign and consolidation shall be completely interoperable.

STRQ511: The IAFIS civil and criminal repositories (fingerprint image, fingerprint vector, and biographical data) after redesign and consolidation shall be completely interoperable, implementing single subject identity and providing a full range of capabilities needed to maintain them.

SFR1884: NCI shall create a pre-conversion copy of International transactions for the NCI Certification File.

SFR1885: NCI shall support an interface to the Special Functions System.

LEG.FR529: IAFIS shall support an interface to the Special Functions System.

SFR1899: NCI shall support the synchronization of internal code tables with corresponding NCIC code tables (e.g., SMT, eye, hair).

STRQ400: The state and country code tables shall be the same in all the different CJIS systems.

SFR1900: NCI shall provide the capability to mark an Identity for notification purposes.

LEG.FR255: IAFIS shall generate a Special Interest Notification when criminal activity occurs on a subject's record marked as Special Interest.

LEG.FR256: IAFIS shall generate a Special Interest Notification when file maintenance occurs on a subject's record marked as Special Interest.

SFR1901: NCI shall provide biographic data as part of the Identity History Summary.

LEG.FR421: IAFIS shall provide biographic information as part of a Subject Criminal History Rap Sheet.

SFR2008: NCI shall provide the capability to maintain limits for the maximum number of candidates to return for all Investigation searches.

SFR2010: NCI shall maintain the original source and date of all data associated with the Identity.

STRQ154: IAFIS shall store a charge classification that indicates if the arrest charge is a felony or misdemeanor.

SFR2027: NCI shall provide the capability to maintain External System Search rules.

BIO.FEAT225: As new fingerprints are provided to the enterprise, the solution shall query the databases (IDENT and IAFIS) to identify whether this person has been seen before.

BIO.FEAT339: The solution shall provide notification of all newly created in-scope IAFIS records, to include biometrics and identifiers to the IDENT system.

SFR2028: NCI shall comply with electronic recordkeeping requirements as outlined in the FBI Electronic Recordkeeping Certification (ERKC) Manual.

SFR2032: NCI shall provide the capability to maintain consolidation rules to support the Identity Consolidation function.

SFR2033: NCI shall support removable media for bulk enrollment of Rap Back information.

SFR2077: NCI shall compare stored latent investigative search results to produce a Post Latent Processing (PLP) Correlation List.

LEG.FR584: IAFIS shall perform a comparison of stored latent investigative search results to produce a Post Latent Processing (PLP) Correlation List.

SFR2078: NCI shall provide the capability to store latent search details.

LEG.FR585: IAFIS shall provide the capability to store latent search details.

SFR2079: NCI shall provide the capability to store all the necessary information for agencies that receive copies of responses in the Computerized Records Sent File.

LEG.FR588: IAFIS shall provide the capability to store all the necessary information for agencies that receive copies of responses in the Computerized Records Sent File.

SFR2080: NGI shall provide Authorized FBI Service Providers with training capabilities.

LEG.FR586: IAFIS shall provide authorized FBI Service Providers with training capabilities.

SFR2081: NGI shall provide Authorized FBI System Administrators with training capabilities.

LEG.FR587: IAFIS shall provide authorized FBI System Administrators with training capabilities.

SFR2172: NGI shall be capable of reporting the number of positive identifications resulting from Tenprint Fingerprint Identification Searches against the NGI Shared Data.

BIO.FEAT89: The solution shall provide the ability to report on the number and types of hits against criminal information based on biometrically-confirmed interactions.

LEG.FR639: IAFIS shall be capable of reporting the number of positive identifications resulting from searches against the IAFIS shared data.

SFR2173: NGI shall be capable of reporting the number of positive identifications resulting from Tenprint Fingerprint Identification Searches against an External System's (e.g., IDENT) Shared Data.

BIO.FEAT89: The solution shall provide the ability to report on the number and types of hits against criminal information based on biometrically-confirmed interactions.

LEG.FR640: IAFIS shall be capable of reporting the number of positive identifications resulting from searches against the IDENT shared data.

SFR2174: NGI shall be capable of reporting the number of Tenprint Fingerprint Identification Searches performed against the records contained in the NGI Shared Data.

BIO.FEAT89: The solution shall provide the ability to report on the number and types of hits against criminal information based on biometrically-confirmed interactions.

LEG.FR641: IAFIS shall be capable of reporting the number of fingerprint searches performed against the records contained in the IAFIS shared data.

SFR2175: NGI shall be capable of reporting the number of Tenprint Fingerprint Identification Searches performed against the records contained in an External System's (e.g., IDENT) Shared Data.

LEG.FR642: IAFIS shall be capable of reporting the number of fingerprint searches performed against the records contained in the IDENT shared data.

SFR2176: Deleted.

SFR2177: Deleted.

SFR2178: NGI shall maintain a Shared Want Image File (SWIF) that is supported by NGI Shared Data updates.

BIO.FEAT106: The solution shall provide agency-to-agency audit trails for data receipt, maintenance, storage, dissemination, and use of shared data.

BIO.FEAT107: The solution shall provide an audit trail of all data capture and update transactions.

LEG.FR646: IAFIS shall maintain a Shared Want Image File (SWIF) that is supported by IAFIS shared data updates.

SFR2179: NGI shall maintain a Shared Want Directory (SWD) that is supported by NGI Shared Data updates.

BIO.FEAT106: The solution shall provide agency-to-agency audit trails for data receipt, maintenance, storage, dissemination, and use of shared data.

BIO.FEAT107: The solution shall provide an audit trail of all data capture and update transactions.

LEG.FR647: IAFIS shall maintain a Shared Want Directory (SWD) that is supported by IAFIS shared data updates.

SFR2180: NGI shall maintain a Shared Want Activity Log (SWAL) that is supported by NGI Shared Data updates.

BIO.FEAT106: The solution shall provide agency-to-agency audit trails for data receipt, maintenance, storage, dissemination, and use of shared data.

BIO.FEAT107: The solution shall provide an audit trail of all data capture and update transactions.

BIO.FEAT279: The solution shall create an Activity Log of removed records.

BIO.FEAT280: The solution shall create an Activity Log of demoted records.

LEG.FR648: IAFIS shall maintain a Shared Want Activity Log (SWAL) that is supported by IAFIS shared data updates.

- SFR2181: NGI shall maintain a Shared Watch Image File that is supported by an External System's (e.g., IDENT) Shared Data updates.**
BIO.FEAT106: The solution shall provide agency-to-agency audit trails for data receipt, maintenance, storage, dissemination, and use of shared data.
BIO.FEAT107: The solution shall provide an audit trail of all data capture and update transactions.
LEG.FR649: IAFIS shall maintain a Shared Watch Image File that is supported by IDENT shared data updates.
- SFR2182: NGI shall maintain a Shared Watch Directory that is supported by an External System's (e.g., IDENT) Shared Data updates.**
BIO.FEAT106: The solution shall provide agency-to-agency audit trails for data receipt, maintenance, storage, dissemination, and use of shared data.
BIO.FEAT107: The solution shall provide an audit trail of all data capture and update transactions.
LEG.FR650: IAFIS shall maintain a Shared Watch Directory that is supported by IDENT shared data updates.
- SFR2183: NGI shall maintain a Shared Watch Activity Log that is supported by an External System's (e.g., IDENT) Shared Data updates.**
BIO.FEAT106: The solution shall provide agency-to-agency audit trails for data receipt, maintenance, storage, dissemination, and use of shared data.
BIO.FEAT107: The solution shall provide an audit trail of all data capture and update transactions.
LEG.FR651: IAFIS shall maintain a Shared Watch Activity Log that is supported by IDENT shared data updates.
- SFR2184: NGI shall support automated scripts that daily check the availability of Shared Data processing servers.**
BIO.FEAT109: The solution shall remain in operation 99% of the time.
LEG.FR652: IAFIS shall support automated scripts that daily check the availability of shared data processing servers.
- SFR2185: NGI shall provide visual alarms to inform system operators or administrators of selected events or violations from the set of system parameters.**
LEG.FR653: IAFIS shall provide visual alarms to inform system operators or administrators of selected events or violations from the set of system parameters.
- SFR2186: NGI shall support shared data terminals or workstations that provide direct access in a controlled environment.**
BIO.FEAT106: The solution shall provide agency-to-agency audit trails for data receipt, maintenance, storage, dissemination, and use of shared data.
BIO.FEAT126: The solution shall provide the ability for human-confirmed 10 print positive identification.
BIO.FEAT143: User groups currently accessing IAFIS shall have access to both IAFIS and IDENT data through the solution.
LEG.FR654: IAFIS shall support shared data terminals or workstations that provide direct access in a controlled environment.
- SFR2248: NGI shall provide the capability to maintain a minimum fingerprint match threshold to support cascaded fingerprint searches of the ULF.**
BIO.FEAT317: The solution shall have the ability to establish a score threshold for latent searching.
BIO.FEAT318: The solution shall have the ability to update a score threshold for latent searching.
- SFR2249: NGI shall provide the capability to maintain a minimum palmprint match threshold to support cascaded palmprint searches of the ULF.**
- SFR2250: NGI shall provide the capability to maintain a minimum facial match threshold to support cascaded searches of the UPF.**
- SFR2251: NGI shall provide the capability to maintain a minimum iris match threshold to support cascaded searches of the UIF.**
- SFR2252: NGI shall provide the capability to maintain minimum fingerprint match thresholds to support cascaded searches of marked SPC files.**
- SFR2253: NGI shall provide the capability to maintain minimum palmprint match thresholds to support cascaded searches of marked SPC files.**
- SFR2254: NGI shall provide the capability to maintain minimum facial match thresholds to support cascaded searches of marked SPC files.**
- SFR2255: NGI shall provide the capability to maintain minimum iris match thresholds to support cascaded searches of marked SPC files.**
- SFR2256: NGI shall perform a cascaded fingerprint search of the ULF using the updated fingerprint composite, in accordance with cascaded search business rules, as a result of a fingerprint composite update.**
- SFR2257: NGI shall perform a cascaded fingerprint search of the marked SPC Files using the updated fingerprint composite, in accordance with cascaded search business rules, as a result of a fingerprint composite update.**
- SFR2258: Deleted.**
- SFR2259: Deleted.**

SFR2260: NGI shall search biometric information against the appropriate unsolved biometric file as a part of a cascaded search.

SFR2261: NGI shall search biometric information against the marked SPC files as part of a cascaded search.

SFR2262: NGI shall apply cascaded search business rules to all cascaded searches.

SFR2263: NGI shall calculate a match score for each candidate resulting from a cascaded search.

SFR2264: NGI shall send an Unsolved Biometric Notification for each candidate resulting from a cascaded search that has a match score above the appropriate cascaded search match threshold.

SFR2265: NGI shall send a Special Population Cognizant Notification for each candidate resulting from a cascaded search that has a match score above the appropriate cascaded search match threshold.

SFR2266: NGI shall provide Authorized FBI Service Providers with supplemental fingerprint and palmprint miss analysis tool capabilities.

SFR2267: NGI shall provide Authorized Contributors with supplemental fingerprint and palmprint information to support miss analysis tools.

SFR2268: NGI shall provide Authorized FBI Service Providers with iris miss analysis tool capabilities.

SFR2269: NGI shall provide Authorized Contributors with iris information to support miss analysis tools.

SFR2270: NGI shall provide Authorized FBI Service Providers with photo miss analysis tool capabilities.

SFR2271: NGI shall provide Authorized Contributors with photo information to support miss analysis tools.

SFR2272: Deleted.

SFR2273: NGI shall record the Iris Search request information to support an iris miss analysis tool.

SFR2274: NGI shall record the Facial Recognition Search request information to support a photo miss analysis tool.

SFR2275: NGI shall have the capability to support fingerprint decision statistical reporting.

SFR2276: NGI shall support supplemental fingerprint and palmprint image quality statistical reporting of NGI Repositories.

SFR2277: NGI shall support palmprint image quality statistical reporting of NGI Repositories.

SFR2278: NGI shall support iris image quality statistical reporting of NGI Repositories.

SFR2279: NGI shall support photo image quality statistical reporting of NGI Repositories.

SFR2280: NGI shall uniquely identify and authenticate Direct Users or processes acting on behalf of users.

LEG.NFR2: IAFIS shall provide direct user identification and authentication for controlling access to IAFIS.

LEG.NFR5: IAFIS shall authenticate the FBI Service Provider using an assigned unique identifier and password during each login attempt.

LEG.NFR9: IAFIS shall require Authorized FBI Service Providers to change their password at the expiration of a time period specified by the System Security Administrator.

LEG.NFR12: IAFIS shall require an FBI Service Provider password to be compliant with the CJIS CAPP.

LEG.NFR13: IAFIS shall prohibit the reuse of the last five passwords used by an individual Authorized FBI Service Provider.

SFR2281: NGI shall identify and authenticate specific devices before establishing a connection.

SFR2282: NGI shall provide the capability for Authorized FBI System Administrators to manage Direct User identifiers by uniquely identifying each user

LEG.NFR6: IAFIS shall provide the System Security Administrator with the ability to enable or disable logon access, change passwords, and specify audit parameters and access privileges for any authorized user.

SFR2283: NGI shall provide the capability for Authorized FBI System Administrators to manage Direct User identifiers by verifying the identity of each user.

LEG.NFR6: IAFIS shall provide the System Security Administrator with the ability to enable or disable logon access, change passwords, and specify audit parameters and access privileges for any authorized user.

SFR2284: NGI shall provide the capability for Authorized FBI System Administrators to manage Direct User identifiers by receiving authorization to issue a user identifier from an appropriate organizational official.

LEG.NFR6: IAFIS shall provide the System Security Administrator with the ability to enable or disable logon access, change passwords, and specify audit parameters and access privileges for any authorized user.

LEG.NFR39: IAFIS shall require a time-out at a terminal or workstation after a specified period of inactivity.

SFR2285: NGI shall provide the capability for Authorized FBI System Administrators to manage Direct User identifiers by ensuring that the user identifier is issued to the intended party.

LEG.NFR4: IAFIS shall provide a unique login capability for each Authorized FBI Service Provider.

LEG.NFR6: IAFIS shall provide the System Security Administrator with the ability to enable or disable logon access, change passwords, and specify audit parameters and access privileges for any authorized user.

SFR2286: NGI shall provide the capability for Authorized FBI System Administrators to manage Direct User identifiers by disabling user identifier after a period of inactivity defined in the System Security Plan.

LEG.NFR6: IAFIS shall provide the System Security Administrator with the ability to enable or disable logon access, change passwords, and specify audit parameters and access privileges for any authorized user.

LEG.NFR27: IAFIS shall log all security related activity (e.g., types of events, date and time of event, User ID, etc.) that occurs within IAFIS in a security audit trail.

SFR2287: NGI shall provide the capability for System Administrators to manage Direct User identifiers by archiving user identifiers.

LEG.NFR6: IAFIS shall provide the System Security Administrator with the ability to enable or disable logon access, change passwords, and specify audit parameters and access privileges for any authorized user.

SFR2288: NGI shall provide the capability for Authorized FBI System Administrators to manage information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by defining initial authenticator content.

LEG.NFR6: IAFIS shall provide the System Security Administrator with the ability to enable or disable logon access, change passwords, and specify audit parameters and access privileges for any authorized user.

SFR2289: NGI shall provide the capability for Authorized FBI System Administrators to manage information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.

LEG.NFR6: IAFIS shall provide the System Security Administrator with the ability to enable or disable logon access, change passwords, and specify audit parameters and access privileges for any authorized user.

SFR2290: NGI shall provide the capability for Authorized FBI System Administrators to manage information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by changing default authenticators upon information system installation.

LEG.NFR6: IAFIS shall provide the System Security Administrator with the ability to enable or disable logon access, change passwords, and specify audit parameters and access privileges for any authorized user.

SFR2291: NGI shall provide feedback to a Direct User during an attempted authentication and that feedback does not compromise the authentication mechanism.

LEG.NFR8: IAFIS shall not display the FBI Service Providers password when entered for authentication purposes.

LEG.NFR10: IAFIS shall not display the FBI Service Provider password when entered as part of a password change.

SFR2292: NGI shall provide capability for the FBI Administrator to manage NGI user accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.

LEG.NFR14: IAFIS shall store FBI Service Provider passwords in encrypted form in a protected personal authenticator file.

LEG.NFR21: IAFIS shall support security administration by the System Security Administrators, each of whom will define and control direct user authentication, profiles, roles, and data access rights as well as workstation functions.

SFR2293: NGI shall provide the capability for the FBI Administrator to monitor NGI user accounts.

SFR2294: NGI Direct user privileges on the information system shall be consistent with the documented user authorizations.

BIO.FEAT139: The solution shall provide access controls based on user permissions.

BIO.FEAT142: The solution shall prevent access to users who have not been authorized to use the system.

BIO.FEAT394: The solution shall implement data control mechanisms for the IDR within each respective system to ensure a requestor is an authorized user.

SFR2295: NGI Indirect user privileges on the information system shall be consistent with the documented user authorizations.

BIO.FEAT139: The solution shall provide access controls based on user permissions.

BIO.FEAT142: The solution shall prevent access to users who have not been authorized to use the system.

BIO.FEAT394: The solution shall implement data control mechanisms for the IDR within each respective system to ensure a requestor is an authorized user.

LEG.NFR17: IAFIS shall provide indirect user identification for controlling access to IAFIS.

SFR2296: NGI access list shall be restricted to, maintained by the system administrator or designated user account manager.

SFR2297: NGI controls shall be implemented to restrict a privileged user's system access to specific terminals when the need for such protection is identified in a risk analysis.

SFR2298: NGI access to security software shall be restricted to security administrators.

LEG.NFR35: IAFIS shall require that all application software satisfy the security features and access control mechanisms of IAFIS.

LEG.NFR43: IAFIS shall provide for security-relevant software to maintain a domain for its own execution that protects itself from external interference or tampering (e.g., by modification of its code or data structures).

SFR2299: NGI separate libraries shall be maintained for program development and maintenance, testing, and production programs.

SFR2300: NGI source code shall be maintained in a separate library.

SFR2301: Access to all NGI programs, including production code, source code, and extra program copies, shall be protected by access control software and operating system features.

LEG.NFR43: IAFIS shall provide for security-relevant software to maintain a domain for its own execution that protects itself from external interference or tampering (e.g., by modification of its code or data structures).

SFR2302: Direct users shall be assigned responsibilities and specific actions to ensure that access controls are implemented correctly.

LEG.NFR15: IAFIS shall enforce access control rules to ensure that system processes, functions, and data objects are accessed only by Authorized Service Providers or Authorized System Administrators, as explicitly defined by assigned role or organizational membership.

LEG.NFR36: IAFIS shall require that all application software satisfy the authentication guidelines of the system.

SFR2303: Indirect users shall be assigned responsibilities and specific actions to ensure that access controls are implemented correctly.

BIO.FEAT139: The solution shall provide access controls based on user permissions.

LEG.NFR36: IAFIS shall require that all application software satisfy the authentication guidelines of the system.

SFR2304: Only specified, authorized, NGI personnel shall have access to the security functions and information of the information system.

LEG.NFR36: IAFIS shall require that all application software satisfy the authentication guidelines of the system.

LEG.NFR95: IAFIS shall prohibit any message from gaining access to privileged system functions without authorization.

SFR2305: Direct user privileges for accounts that have access to information security functions shall operate as documented in accordance with authorization requirements.

SFR2306: NGI shall enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

BIO.FEAT131: The solution shall comply with 28 USC 534, which codifies the FBI's authority to acquire, collect, classify, maintain, preserve, and exchange or disclose criminal history record information.

BIO.FEAT134: The solution shall adhere to the National Crime Prevention and Privacy Compact (42 USC 140 Sec. 14616) that all non-criminal justice access to the Interstate Identification Index (III) must be established through the FBI or SIB.

BIO.FEAT135: The solution shall adhere to the National Crime Prevention and Privacy Compact (42 USC 140 Sec. 14616) requirement that release and use of information obtained through the system for non-criminal justice purposes will be governed by the laws of the receiving States, and the receiving repositories will be required to screen record responses and delete any information that cannot be released legally within the State.

BIO.FEAT142: The solution shall prevent access to users who have not been authorized to use the system.

LEG.NFR40: IAFIS shall prohibit workstations from having any "outside" connection from the IAFIS environment without prior authorization from the System Security Administrator.

SFR2307: NGI shall enforce separation of duties.

SFR2308: NGI functions of significant criticality or sensitivity shall be subject to control by more than one individual.

SFR2309: No Direct user shall have access authorizations or privileges that may allow the user to perform multiple security functions for which the duties should be performed by separate people.

SFR2310: NGI shall not allow a single user to perform multiple functions/roles.

SFR2311: NGI specific actions and responsibilities shall be documented and defined to ensure that the principle of separation of duties is correctly applied within the information system.

SFR2312: NGI shall assign the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.

SFR2313: NGI shall ensure that access rights/privileges correspond to the authorized permissions on access documentation for the specified tasks.

SFR2314: NGI shall apply least privilege concepts in accordance with organizational policy and procedures.

SFR2315: NGI shall assign responsibilities and define specific actions to ensure that the principle of least privilege is correctly applied.

LEG.NFR94: IAFIS shall prohibit any message from circumventing normal processing.

SFR2316: NGI shall enforce a limit of four consecutive invalid login attempts by a Direct user.

LEG.NFR11: IAFIS shall prohibit access to users attempting to login using an invalid or expired login ID or password.

SFR2317: NGI shall automatically lock or disable the Direct user account when the maximum number of unsuccessful attempts is exceeded.

SFR2318: Attempts to login to an NGI Direct user account after it is locked or disabled shall fail.

SFR2319: An NGI System Administrator shall be assigned responsibility and have the capability to define specific actions to ensure that the information system enforces the limit on unsuccessful logon attempts and locks or disables the account when the limit is reached.

LEG.NFR22: IAFIS shall provide the capability for a System Security Administrator deny or allow access to system resources, and monitor local transactions.

SFR2320: NGI shall display to the Direct User an FBI approved, system use notification message before granting system access informing potential users that the user is accessing a U.S. Government information system.

SFR2321: NGI shall display to the Direct User an FBI approved, system use notification message before granting system access informing potential users that system usage may be monitored, recorded, and subject to audit.

SFR2322: NGI shall display to the Direct User an FBI approved, system use notification message before granting system access informing potential users that unauthorized use of the system is prohibited and subject to criminal and civil penalties.

SFR2323: NGI shall display to the Direct User an FBI approved, system use notification message before granting system access informing potential users that use of the system indicates consent to monitoring and recording.

SFR2324: The NGI system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries).

SFR2325: The NGI system use notification message shall remain on the screen until the user takes explicit actions to log on to the information system.

SFR2326: NGI shall notify the Direct user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts

- SFR2327: NGI shall limit the number of concurrent sessions for any Direct user to 1 session only.**
LEG.NFR16: IAFIS shall prohibit Authorized FBI Service Providers from logging into IAFIS more than once concurrently.
- SFR2328: NGI shall prevent further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.**
- SFR2329: NGI shall terminate a Direct user session after 30 minutes or less of inactivity.**
- SFR2330: NGI authentication tokens shall be destroyed when a session terminates.**
- SFR2331: Direct user web browsers shall have only session cookies enabled.**
- SFR2332: NGI shall assign responsibility and specific actions to Authorized FBI System Administrators defined to ensure that session terminations are implemented correctly within the information system.**
- SFR2333: NGI shall provide the capability for the FBI System Security Administrator to monitor and review the all user activities with respect to the**
- SFR2334: NGI shall provide the capability for the FBI System Security Administrator to identify specific user actions that can be performed on the information system without identification or authentication.**
- SFR2335: NGI shall control access to the system based on rules that restrict individual Direct Users according to their system defined roles or organizational membership and need-to-know requirements.**
BIO.FEAT139: The solution shall provide access controls based on user permissions.
LEG.NFR3: IAFIS shall provide direct users, Authorized FBI Service Providers, with access to IAFIS functions, processes and objects based upon assigned user profiles.
SFR2336: NGI shall prevent a requester from executing any process or function not specified in the requester's profile, or implicit in any roles or organizational memberships associated with the identifier.
LEG.NFR33: IAFIS shall ensure that specified data items can only be accessed through transaction routines that correctly enforce the transaction rules.
LEG.NFR33: IAFIS shall ensure that specified data items can only be accessed through transaction routines that correctly enforce the transaction rules.
- SFR2336: NGI shall prevent a requester from executing any process or function not specified in the requester's profile, or implicit in any roles or**
LEG.NFR33: IAFIS shall ensure that specified data items can only be accessed through transaction routines that correctly enforce the transaction rules.
- SFR2337: NGI shall prevent a requester from assuming any role not specified in the requester's profile, or implicit in any roles or organizational memberships associated with the identifier.**
LEG.NFR33: IAFIS shall ensure that specified data items can only be accessed through transaction routines that correctly enforce the transaction rules.
- SFR2338: NGI shall provide transaction accountability for each Direct user activity on the system.**
LEG.NFR34: IAFIS shall ensure that each transaction is consistent with the role(s) assigned to an individual requester.
LEG.NFR35: IAFIS shall require that all application software satisfy the security features and access control mechanisms of IAFIS.
- SFR2339: NGI shall provide transaction accountability for each Indirect user activity on the system.**
LEG.NFR34: IAFIS shall ensure that each transaction is consistent with the role(s) assigned to an individual requester.
- SFR2340: NGI shall require that a response be first matched against an Indirect User message prior to sending the indirect user a response.**
LEG.NFR20: IAFIS shall prohibit automatic responses required by receipt and processing of an external, automated message to IAFIS from being released and returned without first being matched against the message that requested a response.
- SFR2341: NGI shall provide an Administrator role to isolate administrative access.**
LEG.NFR24: IAFIS shall support a direct user login/maintenance function for direct System Security Administrator access.
- SFR2342: NGI shall generate audit records for specific events (for example, account logon events, account management events, directory service access events, object access failures, policy change failures, privilege use failures, and system events.)**
LEG.NFR25: IAFIS shall log all system level activity (e.g. logins, functions, etc) that occurs within IAFIS in a system audit trail.

LEG.NFR28: IAFIS shall provide segment level audit log data in a consolidated format.

SFR2343: NGI shall produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

BIO.FEAT106: The solution shall provide agency-to-agency audit trails for data receipt, maintenance, storage, dissemination, and use of shared data.

BIO.FEAT107: The solution shall provide an audit trail of all data capture and update transactions.

BIO.FEAT280: The solution shall create an Activity Log of demoted records.

SFR2344: NGI shall allocate sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.

SFR2345: In the event of an audit failure or audit storage capacity being reached, NGI shall alert appropriate organizational officials (by audible alert, email, or pager, as determined by local policy) and take the following additional actions: shutdown information system, and/or overwrite oldest audit records, and/or stop generating audit records.

SFR2346: NGI shall provide a warning when allocated audit record storage volume reaches 90% of capacity.

SFR2347: NGI shall provide the System Administrator with the necessary data to review/analyze inappropriate or unusual activity.

SFR2348: NGI shall provide the System Administrator with the necessary data to investigate suspicious activity or suspected violations.

SFR2349: NGI shall provide audit reduction and report generation capability.

SFR2350: NGI shall provide time stamps for use in audit record generation.

LEG.NFR41: IAFIS shall synchronize the master IAFIS clock using an external standard reference time, such as on Coordinated Universal Time (UTC).

SFR2351: NGI shall protect audit information from unauthorized access, modification, and deletion.

LEG.NFR26: IAFIS shall protect the IAFIS audit data from unauthorized access, modification or destruction.

SFR2352: NGI shall protect audit tools from unauthorized access, modification, and deletion.

SFR2353: NGI shall provide the capability to determine whether a given individual created information.

SFR2354: NGI shall provide the capability to determine whether a given individual sent a message.

LEG.NFR92: IAFIS shall require that every received message has a valid ORI, message type and purpose code for which the contributor has authorization.

SFR2355: NGI shall provide the capability to determine whether a given individual approved information [e.g., to indicate concurrence or sign a contract].

SFR2356: NGI shall provide the capability to determine whether a given individual received a message.

SFR2357: NGI shall have the capability to retain online audit logs for 30 days.

SFR2358: NGI shall have the capability to retain offline audit logs for 90 days to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

SFR2359: NGI shall separate user functionality (including user interface services) from information system management functionality.

SFR2360: NGI shall isolate security functions from non-security functions.

SFR2361: NGI shall prevent unauthorized and unintended information transfer via shared system resources.

SFR2362: NGI shall protect against or limit the effects of hardware, software, or communications failures as denial of service attacks.

SFR2363: NGI shall protect against or limit the effects of the lack of communication bandwidth of web sites or internal networks as denial of service attacks.

SFR2364: NGI shall protect against or limit the effects of directed malicious attacks originating internally or externally to DOJ networks as denial of service attacks.

LEG.NFR37: IAFIS shall detect malicious code from entering the IAFIS environment (e.g., automated baseline tools, or virus detection tools).

SFR2365: NGI shall limit the use of resources by priority.

SFR2366: NGI shall monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.

SFR2367: NGI shall protect the integrity of transmitted information.

BIO.FEAT140: The solution shall provide record-based access control.

SFR2368: NGI shall protect the confidentiality of transmitted information.

BIO.FEAT140: The solution shall provide record-based access control.

SFR2369: NGI shall terminate a network connection at the end of a session.

SFR2370: NGI shall establish a trusted communications path between the user and the security functionality of the system.

SFR2371: NGI shall employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.

SFR2372: When cryptography is employed, NGI shall perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.

SFR2373: NGI shall reliably associate security parameters (e.g., security labels and markings) with information exchanged between information systems.

SFR2374: NGI shall comply with organizational certificate policy and certification practice statement for the issuance of public key certificates.

SFR2375: NGI shall monitor the use of mobile code within the information system.

SFR2376: NGI shall control the use of mobile code within the information system.

SFR2377: Upon initial startup or recovery from an interruption in a CJIS criminal support systems [Target of Evaluation (TOE)] service, NGI shall not compromise its resources or those of any connected network.

SFR2378: NGI shall ensure that only authorized Direct users have access to information in printed form or on digital media removed from the information system.

SFR2379: NGI shall have external labels affixed to removable information storage media indicating the distribution limitations and handling caveats of the information.

SFR2380: NGI shall have external labels affixed to information system output indicating the distribution limitations and handling caveats of the information.

SFR2381: NGI shall sanitize information system digital media using approved equipment, techniques, and procedures.

SFR2382: NGI shall track media sanitization actions.

SFR2383: NGI shall document media sanitization actions.

SFR2384: NGI shall sanitize or destroy information system digital media before its disposal or release for reuse outside the organization.

LEG.NFR42: IAFIS shall revoke all authorizations to the information contained within an electronic media prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused storage objects.

SFR2385: NGI shall use DOJ-approved vulnerability scanning tools and techniques to routinely scan the operational system for vulnerabilities.

SFR2386: NGI shall support the use of DOJ-approved vulnerability scanning tools and techniques to scan the operational system when significant new vulnerabilities affecting the system are identified and reported.

SFR2387: NGI shall comply with software usage restrictions.

LEG.NFR35: IAFIS shall require that all application software satisfy the security features and access control mechanisms of IAFIS.

SFR2388: NGI shall enforce explicit rules governing the downloading and installation of software by users.

LEG.NFR43: IAFIS shall provide for security-relevant software to maintain a domain for its own execution that protects itself from external interference or tampering (e.g., by modification of its code or data structures).

SFR2389: Deleted.

SFR2390: Deleted.

SFR2391: Deleted.

- SFR2392:** NGI shall configure the security settings of information technology products to the most restrictive mode consistent with information system operational requirements.
- SFR2393:** NGI shall allow the Administrators to configure NGI to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: **FUNCTIONS** <specified by system owner> **PORTS** <specified by system owner> **PROTOCOLS** <specified by system owner> **SERVICES** <specified by system owner>
- SFR2394:** NGI shall conduct backups of user-level information contained in the information system within a component-defined time period.
- SFR2395:** NGI shall conduct backups of system-level information (including system state information) contained in the information system within a component-defined time period.
- SFR2396:** NGI shall store backup information at an appropriately secured location.
- SFR2397:** NGI shall employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.
- SFR2412:** NGI shall support an interface to IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement.
- BIO.FEAT347: The solution shall require all IAFIS input data to be formatted in accordance with the Interface Control Agreement Jointly held by CJIS and US-VISIT.
- SFR2453:** NGI shall provide the capability to maintain a LESC notification time limit.
- BIO.FEAT401: The solution shall generate a notification to the LESC for custodial (criminal booking) submissions that result in a biometrically-confirmed match in IDENT.
- BIO.FEAT402: The solution shall generate a notification to the LESC for all custodial (criminal booking) submissions with a foreign or unknown place of birth.
- BIO.FEAT403: The notification delivered to the LESC shall follow Nlets User and Technical Guidelines.
- BIO.FEAT404: The solution shall generate a notification to the LESC for national security and certain approved public trust background checks that result in a biometrically-confirmed match in IDENT.
- BIO.FEAT405: The solution shall generate a notification to the LESC for all custodial (criminal booking) submissions that result in a match against an IAFIS record containing a foreign or unknown place of birth.
- BIO.FEAT406: The notification delivered to the LESC shall include the IAFIS identifying number, if available.
- BIO.FEAT407: The solution shall exclude notification to the LESC for submissions that result in a biometrically confirmed match in IDENT against IAFIS provided data, other than KST's, with no associated DHS encounter.
- SFR2457:** NGI shall provide the capability to maintain LESC notification rules.
- BIO.FEAT401: The solution shall generate a notification to the LESC for custodial (criminal booking) submissions that result in a biometrically-confirmed match in IDENT.
- BIO.FEAT402: The solution shall generate a notification to the LESC for all custodial (criminal booking) submissions with a foreign or unknown place of birth.
- BIO.FEAT403: The notification delivered to the LESC shall follow Nlets User and Technical Guidelines.
- BIO.FEAT404: The solution shall generate a notification to the LESC for national security and certain approved public trust background checks that result in a biometrically-confirmed match in IDENT.
- BIO.FEAT405: The solution shall generate a notification to the LESC for all custodial (criminal booking) submissions that result in a match against an IAFIS record containing a foreign or unknown place of birth.
- BIO.FEAT406: The notification delivered to the LESC shall include the IAFIS identifying number, if available.
- BIO.FEAT407: The solution shall exclude notification to the LESC for submissions that result in a biometrically confirmed match in IDENT against IAFIS provided data, other than KST's, with no associated DHS encounter.